Technische Universität Darmstadt

Wirtschaftlichkeit von Zertifizierungsstellen in Deutschland

Vom Fachbereich Rechts- und Wirtschaftswissenschaften
der Technischen Universität Darmstadt genehmigte

Dissertation

zur Erlangung des akademischen Grades Doctor rerum politicarum (Dr. rer. pol.)

Vorgelegt von:
Dipl.-Wirtsch.-Inform. Dipl.-Math. Daniel Walther, Frankfurt/Main

Referent:	Prof. Dr. H. J. Petzold
Korreferenten:	Prof. Dr. Dr. O. Betsch
	Prof. Dr. J. Buchmann

Tag der Einreichung: 10.06.2003
Tag der mündlichen Prüfung: 18.07.2003

Darmstadt, 2003, D17

Inhaltsverzeichnis

Abkürzungsverzeichnis

3DES	Triple-DES
AES	Advanced Encryption Standard
AfA	Absetzung für Abnutzung
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
ARPA	Advanced Research Projects Agency
ASCII	American Standard Code for Information Interchange
B2A	Business-to-Administration
B2B	Business-to-Business
B2C	Business-to-Customer
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BMA	Brandmeldeanlage
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Technologie
BSI	Bundesamt für Sicherheit in der Informationstechnik
C2A	Customer-to-Administration
CA	Certification Authority (Zertifizierungsstelle)
CBC-Mode	Cipherblock Chaining Mode
CC	Common Criteria
CFB-Mode	Cipher Feedback Mode
CRL	Certificate Revocation List (Revozierungsliste)
DDoS	Distributed Denial of Service
DES	Data Encryption Standard

DL	Diskreter Logarithmus
DoS	Denial of Service
DSA	Digital Signature Algorithm
DTA	Datenträgeraustausch
EC	Elliptic Curves (Elliptische Kurven)
ECB-Mode	Electronic Cookbook Mode
EGG	Gesetz zum elektronischen Geschäftsverkehr
E-Mail	Electronic Mail (Elektronische Nachricht)
f.	folgende
FAQ	Frequently Asked Questions (Häufig gestellte Fragen)
FernAbsG	Fernabsatzgesetz
ff.	fortfolgende
GSHB	Grundschutzhandbuch
HBCI	Home Banking Computer Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
Hrsg.	Herausgeber
IBM	International Business Machines
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IMAP4	Internet Message Access Protocol Version 4
inkl.	inklusive
IP	Internet Protocol
ISIS	International Signature Interoperability Specification
ISO	International Standardization Organization
IT	Information Technology (Informationstechnologie)
ITSEC	Information Technology Security Evaluation and Certification
IuKDG	Informations- und Kommunikationsdienste-Gesetz
LWL	Lichtwellenleiter
MIME	Multipurpose Internet Mail Extensions
NEA	Netz-Ersatzanlage

NHV	Niederspannungshauptversorgung
NIST	National Institute of Standards and Technology
NSA	National Security Agency
Nr.	Nummer
OCSP	Online Certificate Status Protocol (Online-Zertifikatsstatusprotokoll)
OSI	Open Systems Interconnection
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public-Key-Infrastruktur
PKIX	Public-Key-Infrastructure X509
POP3	Post Office Protocol Version 3
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFC	Request for Comments
RSA	(Verschlüsselungsalgorithmus nach) Rivest, Shamir und Adleman
S.	Seite
S-HTTP	Secure Hypertext Transfer Protocol
S/MIME	Secure/MIME
SD	Sicherheitsdurchreiche
SHA	Secure Hash Algorithm
SigG	Signaturgesetz
SMTP	Simple Mail Transfer Protocol
Sp.	Spalte
SSL	Secure Sockets Layer
TAN	Transaktionsnummer
TCP	Transmission Control Protocol
TI	Technische Informatik
TU	Technische Universität
TK	Telekommunikation
u.a.	und andere
USV	Unterstromversorgung

VdS	Verband der Schadenverhütung
VerbSchG	Verbraucherschutzgesetz
vgl.	vergleiche
vol.	Volume
VS	Vereinzelungsschleuse
WWW	World Wide Web
XOR	Exklusiv-Oder
zzgl.	zuzüglich

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Problemstellung der Arbeit

Durch die Entwicklung kostengünstiger Kommunikationstechniken, den Preisverfall für Kommunikationsdienstleistungen sowie einen starken Wettbewerb hat sich in den letzten Jahren die Gesellschaft zu einer Kommunikationsgesellschaft entwickelt, in der Informationen immer schneller fließen[1]. Entwicklungsfortschritte im Bereich der Hardware führten zu schnelleren, kleineren und vor allem preiswerteren Geräten. Dadurch wurden moderne Kommunikationstechniken in immer kürzeren Zeitabständen für Privathaushalte erschwinglich. Deutlich wird dies an der sehr schnellen Durchdringung der privaten Haushalte durch das Internet, welche die Verbreitungsgeschwindigkeit von Radio, Fernsehen und Kabelfernsehen bei weitem übertroffen hat. Abbildung 1-1 soll diesen Sachverhalt graphisch veranschaulichen, in der die Verbreitungsgeschwindigkeit von Radio, Fernsehen, Kabelfernsehen und Internet in den Vereinigten Staaten von Amerika eingezeichnet ist[2]. Aus dieser Graphik kann der Zeitraum der Markteinführung bis zum Erreichen von 50 Millionen Teilnehmern abgelesen werden.

---

[1] Vgl. Klau (Globalisierung, 1999), S. 3.

[2] Vgl. Meeker/Pearson (The Internet Retailing Report, 1997), S. 2-2;
Vgl. Röhm (Sicherheit offener Elektronischer Märkte, 2000), S. 2.
Für Nutzerzahlen siehe auch Merz (Electronic Commerce, 1999), S. 36.

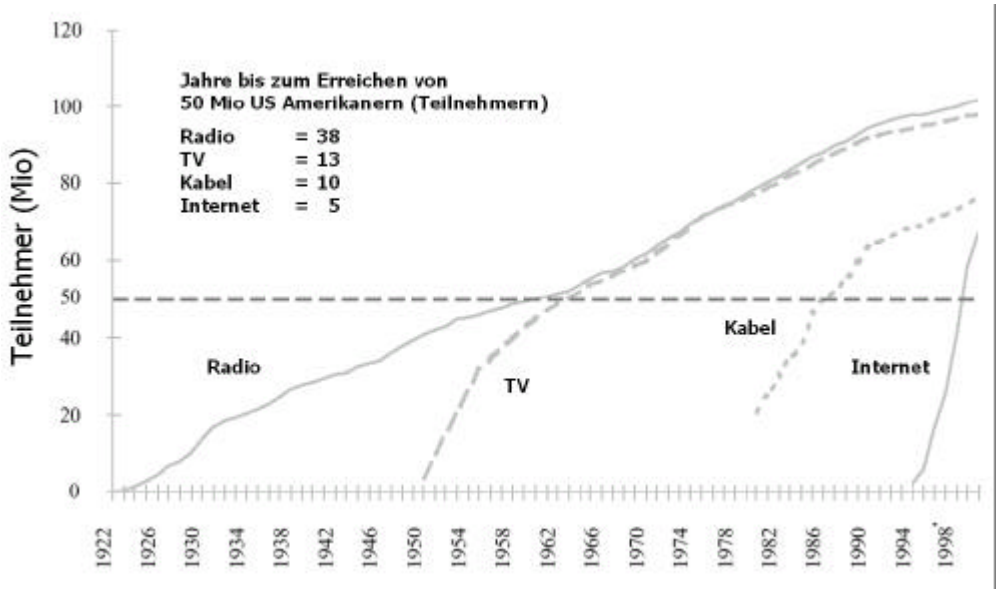

Abbildung 1-1 – Verbreitungsgeschwindigkeit unterschiedlicher Medien in Jahren

Quelle: Meeker/Pearson (The Internet Retailing Report, 1997), S. 2-2

Mittlerweile hat sich das Internet als Infrastruktur für viele Transaktionen im privaten und geschäftlichen Bereich etabliert[3] und dies in fast allen Bereichen des täglichen Lebens. Dabei hat sich das Internet von einem bloßen passiven Informationsangebot zu einem interaktiven Medium[4] entwickelt, das neben der Übertragung von E-Mails elektronischen Handel und die Live-Übertragung von Videodaten ermöglicht.

Einhergehend mit dem Wandel von statischen zu dynamischen und interaktiven Inhalten haben sich die Anforderungen an die zugrundeliegende Infrastruktur verändert[5]. Ergänzend zu dem Sicherheitsproblem, daß die eingesetzten Protokolle des Internets[6] keinerlei Sicherheitsmechanismen zur Authentifikation oder Verschlüsselung vorsehen, können diese auch nicht ohne weiteres nachträglich implementiert werden. Doch dies ist nicht ausschließlich ein technisches Problem; denn

[3] Vgl. Picot (Zehn Eigenschaften der Internet-Ökonomie, 2001), S. 1.

[4] Exemplarisch seien Suchmaschinen angeführt, deren Ergebnisseiten von den Eingaben der Internet-Nutzer abhängen.

[5] Vgl. Zerdick (Die Internet-Ökonomie, 2001), S. 22.

[6] TCP/IP und darauf aufsetzend FTP, HTTP, etc.

während der elektronische Handel Interesse an der tatsächlichen Identität der Käufer hat, möchte der typische Internet-User anonym bleiben[7].

Entscheidend für Veränderungen sind die Auswirkungen des Internets auf das Potential zur Verbesserung von Industriezweigen und Prozessen. Als Industriezweige mit hohem Potential und entsprechend starken Veränderungen sind exemplarisch Verlage und Finanzdienstleister zu nennen.

Durch die neuen Möglichkeiten, die Rechner vor allem in Zusammenhang mit der steigenden Vernetzung bieten, werden immer mehr Geschäftsprozesse den neuen technischen Gegebenheiten angepaßt und elektronisch abgebildet. Vergleichbar mit einer Workflow-Anwendung[8], die über Unternehmensgrenzen hinweg eingesetzt werden soll, treten bei der Implementierung von Prozessen Medienbrüche auf, die ineffizient sind und eine vollständige elektronische Abwicklung verhindern. Als wichtigstes Problem sei an dieser Stelle eine notwendige Unterschrift genannt, die die vollständige elektronische Abbildung des Prozesses verhindert.

Aus diesem Grund wurde 1997 die digitale Signatur durch das erste Signaturgesetz eingeführt. Es sieht Zertifizierungsstellen vor, die eine elektronische Unterschrift einer realen Person zuordnen[9]. Weil diese elektronische Unterschrift in ausgewählten gesetzlich bestimmten Bereichen einer per Hand auf Papier durchgeführten Unterschrift gleichzusetzen ist[10], wurden an die Erstellung der Signatur Bedingungen geknüpft, die äquivalente Sicherheit gewährleisten sollen[11].

---

[7] Vgl. Schneier (Secrets & Lies, 2001), S. 60.

[8] Über Workflows im Telematikprojekt der Bundesvereinigung deutscher Apothekerverbände siehe Brill (Elektronischer Stempel, 2001), S. 546.

[9] Die Signatur kann auch einem Pseudonym zugeordnet werden.

[10] Vgl. Gollan/Meinel (Electronic Signatures, 2000), S. 15.

[11] Dies bedeutet, daß die Unterschrift nicht immer durch eine digitale Signatur ersetzt werden kann. Vielmehr sind durch das Formanpassungsgesetz vom 13.07.2001, BGBl. I 2001 Nr. 35, S. 1542ff., das zum 01.08.2001 in Kraft getreten ist, Formvorschriften u. a. des Bürgerlichen Gesetzbuches an die neuen Technologien angepaßt. Dieses Gesetz ist im Anhang abgedruckt. Für eine Begründung, warum eine Gleichsetzung nicht erfolgen kann, vgl. Langenbach/Ulrich (Elektronische Signaturen, 2002), S. 15ff.

Gerade im elektronischen Bereich wird deutlich, daß Sicherheit niemals absolut, sondern nur relativ sein kann und vor allem hundertprozentige Sicherheit nicht erreichbar ist[12]. Aus diesem Grund sind die Kriterien für Zertifizierungsstellen sehr streng, und dementsprechend schlägt sich deren Erfüllung in hohen Kosten nieder. Da Zertifikate einer Zertifizierungsstelle zur Zeit kostenintensiv sind und ihr Nutzen gering ist[13], bleiben die Teilnehmerzahlen deutlich hinter den Erwartungen zurück[14].

Nach den genannten Überlegungen stellt sich die Frage, ob es möglich ist, Zertifizierungsstellen wirtschaftlich zu betreiben[15].

1.2 Zielsetzung der Arbeit

Diese Arbeit verfolgt zwei Zielsetzungen, die eng miteinander verknüpft sind. Das eine Ziel besteht darin zu überprüfen, ob ein wirtschaftlicher Betrieb einer Zertifizierungsstelle mit hohem Sicherheitsniveau, das heißt beweisbar sicheren Zertifikaten, möglich ist. Das andere beinhaltet die Untersuchung, inwiefern der Betrieb von Zertifizierungsstellen eines niedrigen Sicherheitsniveaus wirtschaftlich sein kann. Dies bedeutet, daß der aus dem Einsatz eines Zertifikates entstehende Nutzen des Teilnehmers seine Kosten übersteigt. Dazu werden die notwendigen Voraussetzungen erläutert und ein allgemeines Verfahren entwickelt, das die Bewertung des erreichten Sicherheitsniveaus mit Blick auf die damit zusammenhängenden Kosten ermöglicht. In Verbindung mit den dargestellten Alternativen im Bereich der Rahmenbedingungen für Zertifizierungsstellen wird ein Weg erarbeitet, der langfristig den wirtschaftlichen Betrieb von Zertifizierungsstellen mit einem hohen Sicherheitsniveau ermöglichen könnte.

---

[12] Vgl. Buchmann (Wie sicher kann Sicherheit sein, 2001), S. 1.

[13] Vgl. Gollan/Meinel (Electronic Signatures, 2000), S. 15.

[14] Vgl. o.V. (Digitale Signatur dank Isis-MTT auf dem Sprung, 2001), S. 37;
vgl. o.V. (Markt noch nicht reif, 2002), S. 1.

[15] Vgl. Fox (Preis der Pioniertat, 2001), S. 62.

1.3 Vorgehensweise der Arbeit

Abbildung 1-2 verdeutlicht die dieser Arbeit zugrundeliegende Vorgehensweise, um die genannten Ziele zu erreichen.

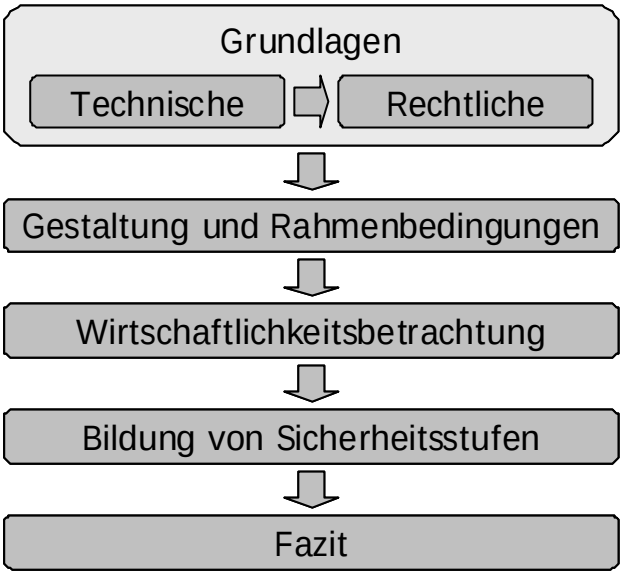

Abbildung 1-2 – Gliederung der Arbeit

Im zweiten Kapitel werden die benötigten technischen Grundlagen erläutert, die die Basis für den Einsatz digitaler Signaturen bilden. Neben den Anforderungen an die elektronische Kommunikation werden kryptographische Grundlagen beschrieben, die zur Erstellung einer digitalen Signatur benötigt werden und eine Einschätzung des damit verbundenen Risikos der Kompromittierung ermöglichen. Im Abschnitt Protokolle wird aufgezeigt, daß der Einsatz kryptographischer Erweiterungen von vorhandenen Protokollen und kryptographischer Protokolle ausreicht, um die geschilderten Anforderungen an die elektronische Kommunikation zu erfüllen. Im Anschluß daran werden der Aufbau und der Einsatz von Zertifikaten dargelegt, als Verbindung von öffentlichen Schlüsseln zu realen Identitäten und damit als Möglichkeit des Austausches öffentlicher Schlüssel über unsichere Netze. Außerdem werden die Wiederherstellung von Schlüsseln und der Einsatz von Mitarbeiterzertifikaten betrachtet. Zum Abschluß des Kapitels werden Zertifizierungsstellen als vertrauenswürdige Dritte vorgestellt und auf die Eigenschaf-

ten von Zertifikatsketten beim Einsatz von Zertifikaten eingegangen. Dies bildet den Ausgangspunkt für Vertrauensverfahren, die im vierten Kapitel erläutert werden.

Im Anschluß an die technischen Grundlagen werden im dritten Kapitel die rechtlichen Grundlagen für Zertifizierungsstellen beschrieben, wobei dieses Kapitel wiederum in zwei Abschnitte aufgeteilt ist. Zum einen werden die Gesetze vorgestellt, die Auswirkungen auf den Aufbau von Zertifizierungsstellen haben, angefangen bei der europäischen Signaturrichtlinie über das deutsche Signaturgesetz und die Signaturverordnung bis zum IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik. Zum anderen werden die Auswirkungen der Gesetze auf die Funktionalität und die Infrastruktur einer signaturgesetzkonformen Zertifizierungsstelle geschildert, die in der Kostenbetrachtung Berücksichtigung finden.

Im vierten Kapitel werden Rahmenbedingungen für Zertifizierungsstellen betrachtet. Aufbauend auf der Beschreibung von Zertifikatsketten im zweiten Kapitel, werden im ersten Abschnitt Vertrauensverfahren für Zertifizierungsstellen erörtert. Denn obwohl im deutschen Signaturgesetz eine zweistufige Hierarchie als Vertrauensverfahren vorgeschrieben ist[16], könnte ein anderes Verfahren unter wirtschaftlichen Gesichtspunkten geeigneter sein. Aus diesem Grund werden ausgehend von Vertrauensverfahren für Personen alternative Verfahren für Zertifizierungsstellen vorgestellt. Im zweiten Abschnitt werden Klassifizierungskriterien für Zertifikate untersucht. Ausgehend von der gegebenen Unterteilung in beweisbar sicher oder nicht wird eine Einteilung nach der Formbedürftigkeit der Transaktion oder nach der Beweiskraft der Zertifikate aus der Literatur diskutiert. Den Kern des Abschnitts bildet jedoch die neu entwickelte Klassifizierung nach dem Kosten-Sicherheits-Verhältnis, bei dem eine mögliche Einteilung direkt aus den denkbaren Zertifizierungsstellen anhand der zugrundeliegenden Kosten und des erreichten Sicherheitsniveaus ermittelt wird. Dieser neue Ansatz betrachtet erstmals nicht nur das Sicherheitsniveau, sondern erlaubt durch die Verknüpfung mit

[16] Vgl. RegTP (Elektronische Signaturen - FAQ, 2002), Frage 15.

den Kosten eine Bewertung, ob zwei verschiedene Sicherheitsniveaus wirtschaftlich sinnvoll zu implementieren sind, oder ob eine Zusammenlegung vorteilhafter wäre. Im dritten Abschnitt findet eine Darstellung der Prozesse einer Zertifizierungsstelle statt, die den Teilnehmern in Rechnung gestellt werden können. Dabei wird ebenfalls berücksichtigt, ob ein Prozeß alleine oder besser in Verbindung mit anderen Prozessen angeboten werden sollte. Aufbauend auf den kryptographischen Grundlagen des zweiten Kapitels werden im vierten Abschnitt Angriffsmöglichkeiten gegen Zertifikate oder mathematische Verfahren beschrieben, um die Wahrscheinlichkeit eines Angriffs bewerten zu können. Den Abschluß des Kapitels bildet eine Bedarfsanalyse, die den Markt für Zertifikate geeignet segmentiert, um die Menge benötigter Zertifikate der unterschiedlichen Sicherheitsniveaus abschätzen zu können. Die sich ergebenden notwendigen Sicherheitsniveaus beeinflussen die Einteilung in Sicherheitsstufen im sechsten Kapitel.

Im fünften Kapitel wird nach einer kurzen Einführung in die verwendete Kostenrechnung eine Betrachtung der Wirtschaftlichkeit einer Zertifizierungsstelle durchgeführt, die im wesentlichen auf einer Kostenbetrachtung von Zertifizierungsstellen unterschiedlicher Sicherheitsniveaus beruht. Als Vorgehensweise bei der Bestimmung der Kosten wird die Zertifizierungsstelle nach den in Kapitel drei erläuterten Infrastrukturkomponenten zerlegt und jeweils sukzessive von minimal nötigen bis durch das Signaturgesetz vorgeschriebenen und damit maximalen Maßnahmen zur Erhöhung der Sicherheit aufgebaut und monetär bewertet. Insbesondere die Bewertung der Sicherheit einzelner Maßnahmen orientiert sich an den im vierten Kapitel beschriebenen Angriffen gegen Zertifizierungsstellen beziehungsweise die angebotenen Zertifikate. Die Summe sämtlicher Kosten der Infrastruktur zuzüglich der Personal- und Materialkosten ergibt die Gesamtkosten einer Zertifizierungsstelle. Um die Wirtschaftlichkeit ermitteln zu können, werden die fixen und variablen Kosten bestimmt und auf ein Zertifikat umgelegt. Mit der Einbeziehung der fixen Kosten können für verschiedene Szenarien an Teilnehmern und damit verkauften Zertifikaten die Kosten eines Zertifikates einer Zertifizierungsstelle errechnet werden. Zusammen mit der Bedarfsanalyse aus dem vorherigen Kapitel und den empirisch ermittelten Marktpreisen eines signaturgesetzkon-

formen Zertifikates kann die Wirtschaftlichkeit einer Zertifizierungsstelle eingeschätzt werden.

Unabhängig von dem bei dieser Analyse erzielten Ergebnis werden im sechsten Kapitel Sicherheitsstufen für Zertifizierungsstellen gebildet, die neben der signaturgesetzkonformen Stufe mit beweisbar sicheren Zertifikaten einen wirtschaftlichen Betrieb ermöglichen können. Dafür wird aufbauend auf dem im vierten Kapitel entwickelten Kosten-Sicherheits-Verhältnis ein Vorgehen entwickelt, das nach diesem Verhältnis optimale Sicherheitsstufen kennzeichnet. Grundlage der Durchführung bilden die im fünften Kapitel ermittelten Kosten, die bei der sukzessiven Erhöhung der Sicherheit einzelner Infrastrukturkomponenten anfallen. Mit Hilfe dieser Daten können im dritten Abschnitt zwei Sicherheitsstufen beschrieben werden, die ein niedriges und ein hohes Sicherheitsniveau darstellen. Die tatsächlich anfallenden Kosten sind an dieser Stelle nicht gesondert zu betrachten, da diese durch die Anwendung des Kosten-Sicherheits-Verhältnisses implizit berücksichtigt sind. Die erhaltenen Stufen bilden jede für sich eine kostenoptimale Implementierung des gewünschten Sicherheitsniveaus. Zum Abschluß des Kapitels wird unter Berücksichtigung der Rahmenbedingungen für Zertifizierungsstellen des vierten Kapitels ein Weg skizziert, der den wirtschaftlichen Betrieb von Zertifizierungsstelle der niedrigen und langfristig den der hohen Sicherheitsstufe mit beweisbar sicheren Zertifikaten ermöglichen könnte. Gleichzeitig werden Voraussetzungen beschrieben, die den zeitlichen Horizont dieser Entwicklung determinieren.

2 Technische Grundlagen

In diesem Kapitel werden die infrastrukturellen Grundlagen beschrieben, die für die Kommunikation im Internet nötig sind. Begonnen wird im ersten Abschnitt mit den generellen Anforderungen an die Kommunikation. Danach folgt eine kurze Einführung in die Kryptographie, die Möglichkeiten bereitstellt, diese Anforderungen zu erfüllen. Im dritten Abschnitt werden der Ablauf internetbasierter Kommunikation anhand der gebräuchlichsten Protokolle beschrieben und verschiedene Erweiterungen zur Nutzung von kryptographischen Methoden erläutert. Im anschließenden vierten Abschnitt geht es um die Verteilung der zuvor beschriebenen Schlüssel und deren Zuordnung mittels Zertifikaten zu Personen oder Webseiten. Mitarbeiterzertifikate im Hinblick auf zusätzliche Anforderungen werden im fünften Abschnitt untersucht und eine auf bekannten Verfahren basierende Lösung vorgestellt. Zum Abschluß werden Zertifizierungsstellen als Aussteller von Zertifikaten und deren weitere Funktionen bei der Bereitstellung einer Public-Key-Infrastruktur (PKI) dargestellt.

2.1 Anforderungen an elektronische Kommunikation

Einige der Anforderungen an die interpersonale Kommunikation sind im täglichen Leben selbstverständlich, wie zum Beispiel die Authentifikation[17]. Es gibt eine Fülle von Merkmalen, an Hand derer eine Erkennung möglich ist. Sitzen sich zwei Menschen beim Gespräch gegenüber, erfolgt eine Erkennung durch das Gesicht, die Haltung, die Stimme, das Verhalten, Besonderheiten der Sprache und die

[17] Vgl. Eckert (IT-Sicherheit, 2001), S. 5.

Kleidung[18]. In anderen Situationen können einzelne Merkmale entfallen und/oder neue hinzukommen. Beim Telefongespräch entfallen viele Erkennungsmerkmale wie Gesicht oder Haltung, andere, wie die Stimme, bleiben jedoch. Hinzu kommt unter anderem die Telefonnummer des Angerufenen, die im allgemeinen fälschungssicher ist. Die Problematik im Internet entsteht durch das gleichzeitige Wegfallen aller Erkennungsmerkmale, so daß eine Authentifikation nicht mehr möglich ist.

Die Kommunikation erfolgt durch die Übertragung von Nachrichten, die jeweils vom Sender an den Empfänger gesendet werden. Im folgenden werden die vier Grundanforderungen an die Kommunikation erläutert, die in sämtlichen möglichen Kombinationen auftreten können[19]. Es handelt sich dabei um Authentifikation, Integrität[20], Vertraulichkeit und Verbindlichkeit[21]. Merkmale wie die Verfügbarkeit werden nicht betrachtet, da sie durch infrastrukturelle oder organisatorische Maßnahmen erreicht werden können[22]. Diese Wertung erfolgt unabhängig davon, daß Verfügbarkeit eine wichtige Rolle in der elektronischen Kommunikation spielt[23]. Dies liegt zum einen daran, daß ohne Verfügbarkeit jede der vorher

---

[18] Vgl. Groth (Stärke multimodaler biometrischer Authentisierung, 2001), S. 1.

[19] Vgl. Schneier (Applied Cryptography, 1996), S. 2;
Vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 3.7.
Für eine ausführliche Betrachtung von Schutzzielen in IT-Systemen siehe Federrath/Pfitzmann (Schutzziele in IT-Systemen, 2000), S. 704ff.

[20] Vgl. Schultz/Proctor/Lien/Salvendy (Usability and Security, 2001), S. 627ff.

[21] Vgl. Buchmann (Wie sicher kann Sicherheit sein, 2001), S. 1;
Vgl. Schneier (Applied Cryptography, 1996), S. 2;
Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 41;
Vgl. Robben (Digitale Signatur, 2000), Internet-Quelle.

[22] Vgl. Thiel (Marktentwicklung im Umfeld digitaler Signaturen, 2000), S. 77;
Vgl. Eckert (IT-Sicherheit, 2001), S. 8.

[23] Vgl. Schneier (Secrets & Lies, 2001), S. 115.

genannten Anforderungen nicht erfüllbar ist, zum anderen daran, daß Angriffe auf die Verfügbarkeit besonders leicht durchführbar sind[24].

Authentifikation

Authentifikation ist ein Verfahren zum Nachweis des berechtigten Empfangs oder der berechtigten Nutzung[25]. Dabei möchte der Sender dem Empfänger eine Nachricht übermitteln und sichergehen, daß diese nur dem adressierten zugänglich ist. Im Gegenzug möchte der Empfänger sicherstellen, daß die Nachricht wirklich von dem in der Nachricht angegebenen Sender versandt wurde.

Integrität

Semantische Integrität bedeutet, daß eine Nachricht unverändert übermittelt wurde[26]. Dies ist die zweite Anforderung, die an eine Nachricht gestellt wird. Der Empfänger hat Interesse daran, kontrollieren zu können, ob es sich bei der empfangenen Nachricht um genau die vom Sender versandte Nachricht handelt, oder ob diese im Nachhinein verändert wurde. Ebenso liegt es im Interesse des Senders, daß der Empfänger die Nachricht nach dem Erhalt nicht mehr verändern kann[27]. Für Sender und Empfänger muß Überprüfbarkeit gegeben sein.

Vertraulichkeit

Vertraulichkeit bedeutet, daß kein Dritter Kenntnis vom Inhalt einer Nachricht erhalten kann[28]. Dies schließt den Fall ein, daß ein Dritter in den Besitz der Nach-

---

[24] DoS (Denial of Service), auch DDoS (Distributed Denial of Service). Mehrere kompromittierte Rechner attackieren ein System, in dem es mit Unmengen von Anfragen überhäuft wird und reguläre Anfragen nicht mehr beantworten kann.

[25] Vgl. Schneier (Applied Cryptography, 1996), S. 2;
Vgl. Eckert (IT-Sicherheit, 2001), S. 5.

[26] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 41;
Vgl. Eckert (IT-Sicherheit, 2001), S. 6.

[27] Ansonsten könnte die Bestellmenge vom Händler zu Lasten des Kunden erhöht werden.

[28] Vgl. Schneier (Applied Cryptography, 1996), S. 2.

richt kommen kann, dies aber keine Rückschlüsse auf den Inhalt der Nachricht ermöglicht. Hierbei ist zu beachten, daß ein Angreifer mittels modernster Abhörmethoden[29] in der Lage ist, jede gewünschte Nachricht zu erhalten, jedoch nicht den eigentlichen Inhalt der Nachricht zu verstehen.
Der Inhalt der Nachricht muß demnach auf eine beliebige Weise verändert werden mit der Maßgabe, daß nur der Empfänger den Inhalt der Nachricht rekonstruieren kann. Dem Empfänger muß die Wiederherstellung der ursprünglichen Nachricht ohne weitere zu übertragende Informationen möglich sein.

Verbindlichkeit

Als letzte Anforderung an die Kommunikation soll die Verbindlichkeit einer Nachricht genannt werden[30]. Verbindlichkeit bedeutet, daß der Empfänger einer Nachricht nachweisen kann, daß diese von einem bestimmten Sender versandt wurde. Insbesondere im Geschäftsleben kommt der Verbindlichkeit große Bedeutung zu, weil zu verhindern ist, daß der Sender abstreiten kann, die Nachricht gesendet zu haben[31]. Aus diesem Grund wird vielfach von Nichtabstreitbarkeit gesprochen[32]. Ebenso muß das Vortäuschen eines mehrfachen Versandes sowohl auf Sender- als auch auf Empfängerseite verhindert werden[33].

2.2 Kryptographische Grundlagen

Ein wichtiges Einsatzgebiet kryptographischer Methoden[34] ist die Chiffrierung von Text und Daten[35]. Dabei wird die ursprüngliche Nachricht mit Hilfe eines Schlüs-

---

[29] Vgl. Schmid (ECHOLON, 2001), S. 25ff.

[30] Vgl. Buchmann (Wie sicher kann Sicherheit sein, 2001), S. 1.

[31] Vgl. Eckert (IT-Sicherheit, 2001), S. 8.

[32] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 3.7.

[33] Nachdem der Empfänger eine Nachricht erhalten hat, die den genannten Kriterien entspricht, könnte er behaupten, die Nachricht doppelt erhalten zu haben, wenn es ihm Vorteile bringt. Dies muß ebenfalls verhindert werden.

[34] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 55.

sels kodiert. Zum Lesen der Nachricht muß diese wiederum durch einen Schlüssel dekodiert werden. Sind dabei die verwendeten Schlüssel identisch oder zumindest leicht aus einander zu berechnen[36], so spricht man von symmetrischer, ansonsten von asymmetrischer Verschlüsselung. Im folgenden werden zuerst beide Verfahren vorgestellt und diskutiert. Danach wird im dritten Abschnitt eine Kombination beider Verfahren beschrieben, bei der jeweils die Schwachstellen des einen durch die Stärken des anderen Verfahrens ausgeglichen werden. Im vierten Abschnitt wird dargestellt, wie Signaturen mit kryptographischen Methoden realisiert werden können und im darauffolgenden Abschnitt, welche verschiedenen Möglichkeiten der Signatur denkbar sind. Im letzten Abschnitt erfolgt eine kurze Einführung in die Kryptoanalyse, die eine Einschätzung ermöglichen soll, wieviel Sicherheit die dargestellten Verfahren bieten können.

Eine weitere Möglichkeit Vertraulichkeit zu erreichen, gegenüber den beschriebenen Verfahren der Verschlüsselung, bietet die Steganographie[37], bei der eine Nachricht in eine unscheinbare Nachricht eingebettet wird und ohne spezielle Kenntnisse nicht als eingebettet erkannt und nicht extrahiert werden kann[38]. Hierbei ist jedoch zu beachten, daß die versteckte Nachricht 0,1 Prozent der Größe der versendeten Nachricht nicht überschreitet[39]. Außerdem kann Vertraulichkeit auf diese Weise nicht garantiert werden, weshalb zusätzlich kryptographische Verfahren auf die versteckte Nachricht angewendet werden müssen.

---

[35] Vgl. Selke (Kryptographie, 2000), S. 33.

[36] Vgl. Schneier (Applied Cryptography, 1996), S. 4;
Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 56.

[37] Vgl. Dittmann (Digitale Wasserzeichen, 2001), S. 14;
Vgl. Selke (Kryptographie, 2000), S. 119.

[38] Vgl. Eckert (IT-Sicherheit, 2001), S. 165.

[39] Vgl. Dittmann (Digitale Wasserzeichen, 2001), S. 52;
Vgl. ebenda, S. 74.
Eckert (IT-Sicherheit, 2001), S. 170 gibt eine Manipulation des least significant bit jedes Bytes an, so daß 1/8 = 12,5% der Daten Nutzdaten wären. In diesem Fall wären die Daten jedoch nicht mehr versteckt, da jedes mögliche Bit genutzt würde. Aus diesem Grund liegt die tatsächlich mögliche Datenrate deutlich darunter.

2.2.1 Symmetrische Verschlüsselung

Ein einfacher symmetrischer Verschlüsselungsalgorithmus ist die Caesar-Chiffre, bei der jeder Buchstabe des Alphabets durch den n Buchstaben später folgenden ersetzt wird[40]. Die Dekodierungsfunktion benutzt offensichtlich denselben Schlüssel n, da jeder Buchstabe durch den n Buchstaben früheren ersetzt werden muß.
Dieses und andere klassische Verfahren früherer Zeit folgen einer einfachen Konstruktion, damit ein Mensch oder ein einfaches mechanisches Gerät die Ver- und Entschlüsselung durchführen konnten[41]. Ein Angreifer konnte jedoch Informationen über die Sprache nutzen, daß beispielsweise im deutschen auf ein c fast immer ein h oder k folgt, um die Nachricht zu entschlüsseln. Dies kann jedoch erschwert werden, indem die Ersetzung nicht zeichenweise durchgeführt, sondern gleich ein längerer Block von Zeichen ersetzt wird. Bei diesen Verfahren, den Blockchiffren, schlägt sich das Vertauschen eines Zeichens innerhalb eines Blockes nicht in einem vertauschten Zeichen innerhalb des Ergebnisblocks, sondern in einem komplett neuen Block nieder[42].
Ein Verschlüsselungsverfahren, das aus diesen Blockchiffren eine Chiffrierung für beliebig lange Texte entwickelt, ist der Electronic Cookbook Mode (ECB-Mode)[43], bei dem gleiche Klartextblöcke gleiche Chiffretextblöcke zur Folge haben. Die Einfachheit dieser Methode wird anhand Abbildung 2-1 deutlich.

---

[40] Nach z folgt wieder der Buchstabe a.

[41] Exemplarisch seien Cäsar-Chiffre, Substitutions-Chiffren, Permutations-Chiffren, Vignere-Chiffre, Vernam-Chiffre genannt. Eine Beschreibung bietet Schmeh (Kryptographie, 2001), S. 54ff und Wobst (Abenteuer Kryptologie, 1998), S. 29ff.

[42] Vgl. Selke (Kryptographie, 2000), S. 42f

[43] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 64;
Vgl. Smith (Internet Kryptographie, 1998), S. 56.

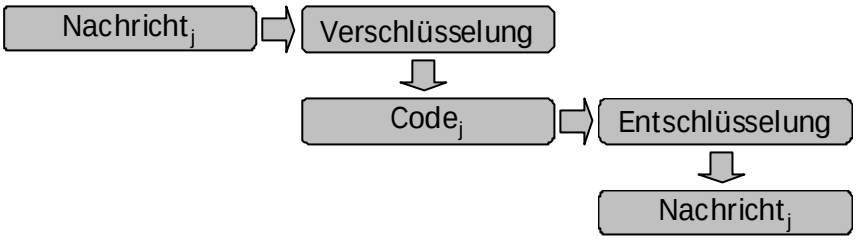

Abbildung 2-1 – Verschlüsselung nach dem ECB-Mode

Um diesen Nachteil[44] zu beseitigen, hängt beim Cipherblock Chaining Mode (CBC-Mode)[45] die Verschlüsselung nicht nur vom Schlüssel, sondern zusätzlich von den vorherigen Blöcken ab. Ein Übertragungsfehler beeinflußt jedoch nur den betroffenen und den darauf folgenden Block, wie in Abbildung 2-2 deutlich wird. Bei diesem Algorithmus kann es zu Effizienzproblemen kommen, da der Empfänger erst mit der Entschlüsselung des Blocks beginnen kann, wenn der Sender einen vollständigen Schlüsseltextblock erzeugt und versandt hat.

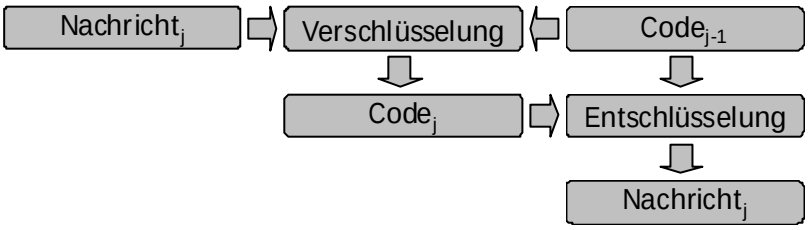

Abbildung 2-2 – Verschlüsselung nach dem CBC-Mode

Abhilfe schafft hier der Cipher Feedback Mode (CFB-Mode)[46], der allerdings aufgrund des gemeinsam benutzten Schlüssels beim Ver- und Entschlüsseln bei asymmetrischen Verfahren nicht mehr eingesetzt werden kann.

Am weitesten verbreitet in der heutigen Software ist der sogenannte Data Encryption Standard (DES)[47], der Mitte der siebziger Jahre unter Beteiligung von

---

[44] Die genaue Begründung, daß dies ein Nachteil ist, folgt im Kapitel Kryptoanalyse.

[45] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 65;
Vgl. Smith (Internet Kryptographie, 1998), S. 56.

[46] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 68;
Vgl. Smith (Internet Kryptographie, 1998), S. 57.

International Business Machines (IBM) und des amerikanischen Geheimdienstes National Security Agency (NSA) entwickelt wurde und zu den Blockchiffren zählt. Zu den Entwurfszielen gehörten damals leichte Verständlichkeit, wirtschaftliche Umsetzbarkeit, Berechenbarkeit mit einem vertretbaren Aufwand, hochgradige Sicherheit und öffentliche Verfügbarkeit. Abbildung 2-3 zeigt eine Darstellung der internen Blockchiffre des DES.

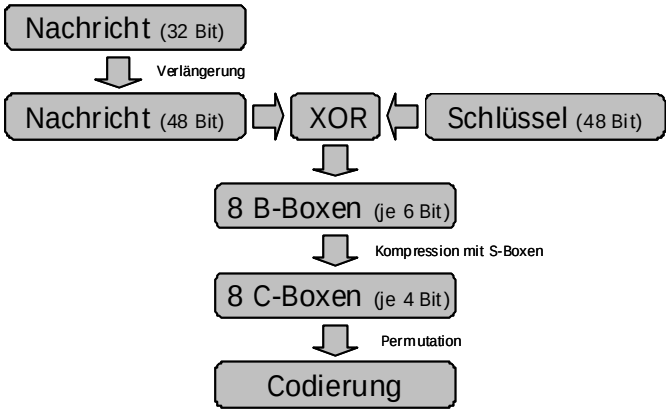

Abbildung 2-3 – Interne Blockchiffre des DES

Quelle: Buchmann (Einführung in die Kryptographie, 2001), S. 98.

Aufgrund der Berechnung, die mit Permutationen und XOR-Verknüpfungen auskommt, ist der Algorithmus enorm schnell und kann zudem leicht in Hardware abgebildet werden. Dies erlaubt eine Erweiterung auf den Tripple-DES (3DES)[48], bei dem der DES drei mal angewendet wird und sich die Schlüssellänge auf 112 Bits erhöht. Dabei wird zunächst der Klartext mit dem ersten 56 Bit Schlüssel verschlüsselt, bevor er mit dem zweiten 56 Bit Schlüssel entschlüsselt und wieder mit dem ersten verschlüsselt wird[49].

---

[47] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 96;
Vgl. Schmeh (Kryptographie, 2001), S. 69.

[48] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 103.

[49] Vorteil dieser Vorgehensweise ist die Tatsache, daß eine Anwendung mit zwei identischen Schlüsseln einer Anwendung eines einfachen DES entspräche.
Vgl. Schmeh (Kryptographie, 2001), S. 82.

Obwohl es am Anfang Kritik[50] am DES gab, muß festgestellt werden, daß die oben genannten Ziele tatsächlich erreicht worden sind. Allerdings kann die Schlüssellänge von 56 Bit, bei einer Blocklänge von 64 Bit, aufgrund der kryptographischen Entwicklungen und der enormen Steigerungen der Rechengeschwindigkeit nach Moore's Law[51] nicht mehr als sicher angesehen werden.
Aus diesem Grund mußten andere symmetrische Verschlüsselungsalgorithmen gefunden werden. Eine Übersicht der bekannten Verfahren findet sich in Abbildung 2-4.

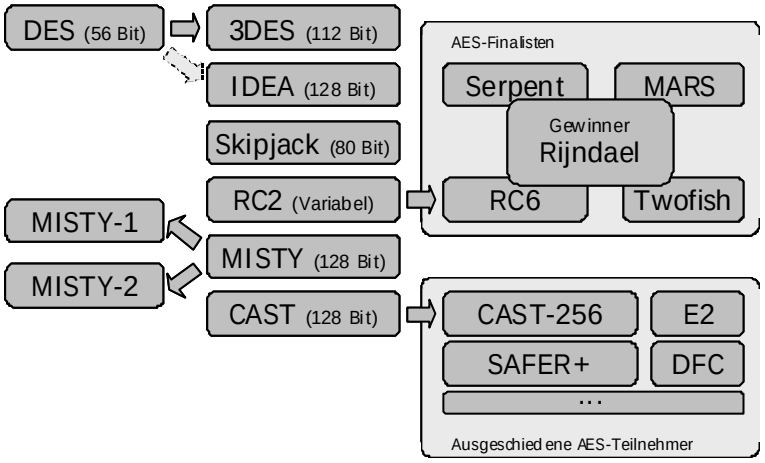

Abbildung 2-4 – Symmetrische Verschlüsselungsverfahren

Die nächste Generation der symmetrischen Verschlüsselungsalgorithmen bildet der Advanced Encryption Standard (AES)[52]. Dieser sollte im Rahmen eines 1997 ausgeschriebenen öffentlichen Wettbewerbs der amerikanischen Normierungsbehörde National Institute of Standards and Technology (NIST)[53] ermittelt werden, bei dem Rijndael[54] im Jahre 2001 aus 15 Kandidaten als Sieger hervorging. Er

[50] U.a. blieben die Entwurfskriterien für die S-Boxen, dem sicherheitsrelevanten Teil von DES zunächst geheim. Vgl. Wobst (Abenteuer Kryptologie, 1998), S. 125.

[51] Alle 18 Monate verdoppelt sich die Rechengeschwindigkeit verfügbarer Prozessoren bei gleichzeitiger Halbierung der benötigen Fläche. Vgl. Moore (Components onto integrated circuits, 1965), S. 115, 116.

[52] Vgl. Schmeh (Kryptographie, 2001), S. 89.

[53] Vgl. Schneier (Applied Cryptography, 1996), S. 600.

[54] Vgl. Welschenbach (Rijndael - Nachfolger des DES, 2001), S. 318.

verfügt, wie gefordert, über eine Blocklänge von 128 Bit und eine Schlüssellänge von 128, 192 oder 256 Bit. Weitere Kriterien des Wettbewerbs waren die freie Verfügbarkeit und eine höhere Geschwindigkeit als 3DES[55]. Die Sicherheitsanforderungen wurden dadurch gewährleistet, daß alle Algorithmen mehrere Monate intensiv öffentlich[56] untersucht und keinerlei Schwachstellen gefunden wurden.

2.2.2 Asymmetrische Verschlüsselung

Das zentrale Problem symmetrischer Verschlüsselungsalgorithmen stellt die Schlüsselverteilung dar, da je zwei Kommunikationspartner einen gemeinsamen Schlüssel benötigen. Zum einen muß der Schlüssel über einen sicheren Kanal ausgetauscht werden, was insbesondere bei weit entfernten Kommunikationspartnern schwierig ist. Zum anderen erhöht sich die Anzahl der benötigten Schlüssel quadratisch[57] zur Anzahl der Teilnehmer.

Eine Möglichkeit der Behebung bestünde darin, die gesamte Kommunikation über eine zentrale Stelle laufen zu lassen, so daß jeder Teilnehmer nur noch einen geheimen Schlüssel mit dieser Stelle austauschen muß. Vorraussetzung dafür ist allerdings, daß jeder Teilnehmer der zentralen Stelle vertraut, da diese jeglichen Nachrichtenverkehr mitlesen könnte. Außerdem müßten alle Schlüssel sicher gespeichert werden und der Datenfluß von und zu dieser Stelle muß ausreichend schnell sein. Die Gefahr, daß ein Nadelöhr entstünde, wäre groß, da das verschlüs-

---

[55] Vgl. Nechvatal/Barker/Bassham/Burr/Dworkin/Foti/Roback (Advanced Encryption Standard (AES), 2000), S. 12;
Vgl. Schmeh (Kryptographie, 2001), S. 89.

[56] Um Angriffe auf Verschlüsselungsverfahren zu erschweren, kann das verwendete Verfahren geheim gehalten werden. Ein Angreifer kann jedoch Rückschlüsse aus abgefangenen Nachrichten ziehen oder jemanden zur Preisgabe der Informationen überreden, so daß es unklar ist, ob Geheimhaltung funktioniert.

[57] Zwei Teilnehmer brauchen 1 Schlüssel. Pro hinzukommendem Teilnehmer kommt ein Schlüssel zu jedem schon existierenden Teilnehmer hinzu. Die Summe der Schlüssel von n Teilnehmern ist demnach die Summe der natürlichen Zahlen von 1 bis n-1, also n * (n - 1) / 2 oder anders $n^2 / 2 – n / 2$.

selte Kommunikationsaufkommen zum einen mit der Teilnehmerzahl und zum anderen mit dem Sicherheitsbedürfnis der Teilnehmer wachsen würde.

Ein Verfahren, das die eben genannten Schwachstellen kompensiert, wurde 1976 von den Amerikanern Witfield Diffie und Martin Hellman veröffentlicht[58]. Beim Diffie-Hellman-Verfahren werden geheime Schlüssel über unsichere Leitungen ausgetauscht. Darauf basiert das El-Gamal-Verfahren[59], bei dem zum Ver- und Entschlüsseln unterschiedliche Schlüssel verwendet werden, wobei es nur mit unverhältnismäßig hohem Aufwand möglich ist, einen Schlüssel aus dem zugehörigen anderen zu berechnen[60]. Es werden der private oder geheime, zum Entschlüsseln verwendete, und der öffentliche, zum Verschlüsseln verwendete, Schlüssel unterschieden[61]. Aus diesem Grund wird asymmetrische Verschlüsselung als Public-Key-Verschlüsselung bezeichnet. Möchte der Sender dem Empfänger eine vertrauliche Nachricht zukommen lassen, so benötigt er zunächst den öffentlichen Schlüssel des Empfängers. Dieser kann jedoch einfach veröffentlicht werden, beispielsweise in einer Zeitung oder auf einer Webseite, oder auf einem unsicheren Kanal übertragen werden, da ein Angreifer keine Vorteile aus dem Schlüssel ziehen kann. Der Empfänger kann die Nachricht nach Erhalt mit seinem, nur ihm bekannten, privaten Schlüssel entschlüsseln. Daher ist kein anderer in der Lage, die Nachricht zu entschlüsseln. Das Problem des Schlüsselaustausches ist damit auf elegante Art und Weise gelöst.

---

[58] Vgl. Diffie/Hellmann (New Directions in Cryptography, 1976), S. 644ff.
Merkle reichte zeitgleich eine Arbeit zum gleichen Thema ein.
Vgl. Wobst (Abenteuer Kryptologie, 1998), S. 150;
Vgl. Selke (Kryptographie, 2000), S. 63.

[59] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 129f.

[60] Unverhältnismäßig hoher Aufwand bedeutet in diesem Fall, daß ein Angreifer im Durchschnitt die Hälfte alle Schlüssel durchprobieren müßte, um den gewünschten zu erhalten. Außerdem ist diese Menge so groß, daß es selbst mit sehr vielen schnellen Computern zu lange dauern würde. Zum Zeitpunkt der Ermittlung des gesuchten Schlüssels wäre er für den Angreifer wertlos.

[61] Vgl. Schmeh (Kryptographie, 2001), S. 95.

Das erste und bis heute das wichtigste Verfahren Public-Key-Verfahren ist das nach seinen Erfindern Ron Rivest, Adi Shamir und Len Adleman benannte RSA-Verfahren[62]. Hierbei besteht der öffentliche Schlüssel aus dem Zahlenpaar (n,e), und der private Schlüssel ist die Zahl d. Als wichtiges Ergebnis kann gezeigt werden, daß die Bestimmung des privaten Schlüssels d aus dem öffentlichen (n,e) genauso schwierig ist, wie die Zerlegung von n in seine Primfaktoren[63]. Damit ist die Bedingung erfüllt, daß man einen Schlüssel nicht einfach aus dem anderen berechnen kann.
Vereinfacht dargestellt wird eine Nachricht m mit dem öffentlichen Schlüssel folgendermaßen verschlüsselt:

$$c = m^e \bmod n.$$

Die erhaltene verschlüsselte Nachricht c kann folgendermaßen entschlüsselt werden:

$$m = c^d \bmod n.$$

Durch die Berechnungsvorschrift wird deutlich, daß im Gegensatz zum DES oder AES-Verfahren, bei dem nur einfache XOR-Operationen und Permutationen benutzt werden, durch die erforderlichen Multiplikationen[64] ein wesentlich höherer Rechenzeitbedarf anfällt. Allein durch die schnelle Exponentiation[65] ist es überhaupt möglich, diese Berechnungen durchzuführen, da bei einem 1024-Bit-RSA-Schlüssel die Exponenten d und e im Bereich 512-Bit liegen, was einer Zahl mit circa 150 Dezimalstellen entspricht.

---

[62] Vgl. Rivest/Shamir/Adleman (A Method for Obtaining Public-Key Cryptosystems, 1978), S. 1ff.

[63] Für eine genauere Darstellung, vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 115ff.

[64] Aufwand Faktor 4 gegenüber einer einfachen Operation wie Addition, XOR, Permutation.

[65] Auch Square-and-Multiply-Technik genannt.

Eine andere Möglichkeit der Public-Key-Kryptographie bieten elliptische Kurven (Elliptic Curves, EC). Im Gegensatz zum RSA-Verfahren basiert die Schwierigkeit der Lösung des Problems jedoch nicht auf dem Faktorisierungsproblem, sondern auf dem Diskreten Logarithmus-Problem (DL-Problem)[66]. Obwohl Arithmetik innerhalb elliptischer Kurven aufwendiger ist als die modulare Arithmetik beim RSA-Verfahren, bieten diese Effizienzvorteile, da die verwendeten Zahlen wesentlich kleiner sein können. Hier lassen sich vom Sicherheitsstandpunkt aus etwa 1024-Bit-Zahlen beim RSA-Verfahren mit 163-Bit-Zahlen beim EC-Verfahren vergleichen[67].

Hierbei ist zu bemerken, daß sich diese Probleme vermutlich orthogonal zueinander verhalten, das heißt, eine Lösung des Faktorisierungsproblems hat noch nicht die Lösung des DL-Problems zur Folge und umgekehrt[68].

2.2.3 Kombination von Verfahren

Der Geschwindigkeitsfortschritt bei elliptischen Kurven gegenüber dem RSA-Verfahren reicht aus, um beispielsweise bei Smart-Cards auf den Koprozessor verzichten zu können[69]. Noch effizienter in der Berechnung sind symmetrische Verschlüsselungsalgorithmen, exemplarisch sei der Geschwindigkeitsfaktor von 3DES gegenüber RSA aufgeführt, der bei einer Implementierung in Software auf 10 geschätzt wird[70]. Aus Gründen der Bedienbarkeit folgt deshalb, daß bei großen Datenmengen oder notwendigerweise schnellen Antwortzeiten kein asymmetrisches Verfahren zum Einsatz kommen sollte.

---

[66] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 195.

[67] Vgl. Buchmann (Faktorisierung großer Zahlen, 1999), S. 196.

[68] Dies ist nicht bewiesen. Ohne die Kenntnis der Algorithmen läßt sich ein Beweis schwer führen.

[69] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 196.

[70] Vgl. Selke (Kryptographie, 2000), S. 76

Da der Einsatz eines symmetrischen Verfahrens einen geheimen Schlüssel voraussetzt[71], der beiden Kommunikationspartnern bekannt ist, muß dieser vorher mit Hilfe eines asymmetrischen Verfahrens ausgetauscht werden[72]. Dieser Sitzungsschlüssel kann frei gewählt und damit zufällig erzeugt werden; nach Abschluß der Sitzung wird er nicht mehr benötigt[73].

Diese Kombination der symmetrischen und asymmetrischen Verfahren, die hybrides Verfahren genannt wird, verbindet somit die Vorteile beider Verfahren miteinander[74]. Allerdings muß beachtet werden, daß dieses kombinierte Verfahren nicht skalierbar ist[75]. Während bei RSA-Verfahren durch einfache Verlängerung der Schlüssellänge die Sicherheit erhöht werden kann[76], ist dies bei symmetrischen Verfahren wie DES oder AES nicht der Fall, da diese, wie oben erwähnt, nur für bestimmte Schlüssellängen ausgelegt sind. Eine Verlängerung der Schlüssellänge beim RSA durch den Faktor 1,1 hat eine Vergrößerung des Schlüsselraumes um etwa den Faktor 7 zur Folge[77]. Ein weiteres Problem kann bei der Übertragung von Nachrichten weniger Bytes entstehen[78], wenn durch die ständige Übertragung eines neuen Sitzungsschlüssels, mit der Blocklänge des asymmetrischen Verfahrens, die Nachrichten aufgebläht werden.

2.2.4 Signaturen

Eine Signatur eines Dokumentes besteht aus zusätzlichen Informationen, die Dritte genau einer bestimmten Person zuordnen können[79]. Im Falle eines elektroni-

---

[71] Vgl. Schmeh (Kryptographie, 2001), S. 94;
Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 56.

[72] Vgl. Schmeh (Kryptographie, 2001), S. 115.

[73] Vgl. Selke (Kryptographie, 2000), S. 77.

[74] Vgl. Schmeh (Kryptographie, 2001), S. 115.

[75] Vgl. Selke (Kryptographie, 2000), S. 75.

[76] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 121.

[77] Vgl. Selke (Kryptographie, 2000), S. 75

[78] Als wichtigste Anwendung mit diesen Eigenschaften ist die vollautomatisierte Kommunikation zwischen zwei Computern zu nennen.

[79] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 177.

schen Dokumentes handelt es sich um zusätzliche Daten, bei denen der Ersteller der Signatur nachweisen kann, daß nur er diese aus dem entsprechenden Dokument erstellt haben kann[80].

Asymmetrische Verfahren verfügen über den Vorteil, daß die Verschlüsselung sowohl über den öffentlichen als auch den privaten Schlüssel erfolgen kann. Erfolgt die Verschlüsselung mittels des privaten Schlüssels, ist von einer Vertraulichkeit jedoch nicht auszugehen, da jeder mit dem öffentlichen Schlüssel die Nachricht entschlüsseln kann. Jedem, der eine Nachricht entschlüsselt, ist jedoch implizit klar, daß diese Nachricht nur vom Besitzer des privaten Schlüssels erzeugt werden konnte, der zum entsprechenden öffentlichen paßt, da dieser geheim ist[81]. Damit wird deutlich, daß sämtliche asymmetrischen Verfahren zum Verschlüsseln und zum Signieren verwendet werden können[82].

Neben dem RSA-Signaturverfahren[83] existieren weitere Signaturverfahren[84], exemplarisch seien das ElGamal-Signaturverfahren[85] oder der 1991 von der amerikanischen Normierungsbehörde National Institute of Standards and Technology vorgeschlagene und später zum Standard erklärte Digital Signature Algorithm (DSA)[86] erwähnt[87].

---

[80] Vgl. Eckert (IT-Sicherheit, 2001), S. 251.

[81] Bertsch (Digitale Signaturen, 2001), S. 18.

[82] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 182.

[83] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 178ff;
Vgl. Schmeh (Kryptographie, 2001), S. 119.

[84] Für die Konstruktion von Signaturverfahren aus Public-Key-Verschlüsselungsverfahren vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 182;
Vgl. Schmeh (Kryptographie, 2001), S. 127, 237ff.
Geeignete Algorithmen aus Sicht des BSI in RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 92.

[85] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 182ff;
Vgl. Schmeh (Kryptographie, 2001), S. 120.

[86] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 187ff.

[87] Vgl. Schneier (Applied Cryptography, 1996), S. 483.

Ein auf die oben beschriebene Weise implementiertes Signaturverfahren hat den Nachteil, daß die vollständige Nachricht mit dem privaten Schlüssel verschlüsselt werden muß. Um diesen zeitaufwendigen Vorgang zu umgehen, werden Hashfunktionen benutzt. Darunter soll eine Funktion verstanden werden, die beliebig lange Nachrichten auf Nachrichten fester Länge abbildet. Dabei darf die Funktion jedoch auf keinen Fall injektiv sein, noch darf es mit vertretbarem Aufwand möglich sein, zwei Nachrichten zu finden, die auf die gleiche Nachricht abgebildet werden[88].

Ein ganze Reihe von Hashfunktionen stammen von Ron Rivest, einem der Erfinder des RSA-Algorithmus. Bei seinen Verfahren MD2, MD4[89] und MD5[90] wurden jedoch Schwächen gefunden, weshalb sie nicht mehr eingesetzt werden sollten[91]. Eine Weiterentwicklung von MD5 ist der US Secure Hash Algorithm (SHA), den die NSA im Auftrag der NIST entwickelt hat und der heute üblicherweise in der Version SHA-1[92] eingesetzt wird, nachdem Schwächen in der ursprünglichen Version, SHA-0, entdeckt wurden[93]. Der erzeugte Hashwert hat eine Länge von 160 Bit. Eine andere Hashfunktion ist RIPEMD-160[94] von Hans Dobbertin, Antoon Bosselaers und Bart Preneel, die eine Weiterentwicklung von RIPEMD, des RIPE-Projektes der EU darstellt, welches wiederum von MD4 beeinflußt wurde. RIPEMD-160 erzeugt ebenfalls 160 Bit Hashwerte, beschrieben sind allerdings zusätzliche Verfahren für 128, 192 und 256 Bit. Mit beiden Verfahren lassen sich

---

[88] Buchmann (Einführung in die Kryptographie, 2001), S. 167ff.

[89] Vgl. Rivest (MD4 - RFC 1320, 1992), Internet-Quelle.

[90] Vgl. Rivest (MD5 - RFC 1321, 1992), Internet-Quelle;
Vgl. Schneier (Applied Cryptography, 1996), S. 435ff.

[91] Vgl. Wobst (Abenteuer Kryptologie, 1998), S. 256;
Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 173.

[92] Vgl. Eastlake/Jones (SHA1 - RFC 3174, 2001), Internet-Quelle;
Vgl. Eckert (IT-Sicherheit, 2001), S. 243.

[93] Vgl. RSA (What are SHA and SHA-1?, 2002), Internet-Quelle.

[94] Vgl. Dobbertin/Bosselaers/Preneel (The hash function RIPEMD-160, 2001), Internet-Quelle. Ebenso, wie SHA-1, bis 2003 aus Sicht des BSI geeignet. Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 91.

große Datenmengen schnell verarbeiten. Auf einem aus heutiger Sicht langsamen Pentium 90 immerhin 5 Megabyte pro Sekunde, wobei RIPEMD-160 etwa 20% langsamer ist als SHA-1[95]. Eine Übersicht über Hashalgorithmen[96] bietet Abbildung 2-5.

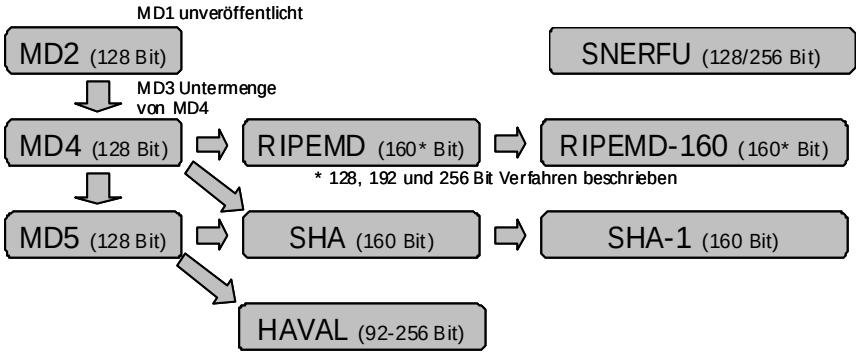

Abbildung 2-5 – Hashalgorithmen im Überblick

Durch das Hashen einer Nachricht entfällt die Notwendigkeit, die komplette Nachricht zu signieren, da der Hashwert per Definition ebenso einmalig ist wie die Nachricht selbst[97]. Zum Signieren einer Nachricht wird deshalb zuerst der Hashwert der Nachricht gebildet und anschließend signiert. Dann wird die Nachricht zusammen mit dem Hashwert an den Empfänger versendet. Dieser trennt den Hashwert von der Nachricht und entschlüsselt diesen. Danach bildet er selbst den Hashwert der Nachricht und kann damit überprüfen, ob beide Werte identisch sind. Ist dies der Fall, so kann der Empfänger sicher sein, daß die Nachricht von dem Sender stammt, der den Hashwert signiert hat. Dieser wurde durch die Entschlüsselung mit dem öffentlichen Schlüssel verifiziert. Das Verfahren wird anhand Abbildung 2-6 verdeutlicht.

---

[95] Vgl. Dobbertin/Bosselaers/Preneel (The hash function RIPEMD-160, 2001), Internet-Quelle. In dieser Quelle finden sich zusätzlich Zahlen zu anderen Verfahren, beispielsweise MD4.

[96] Vgl. Garfinkel/Spafford (Practical Unix and Internet Security, 1996), Kapitel 6.

[97] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 167.

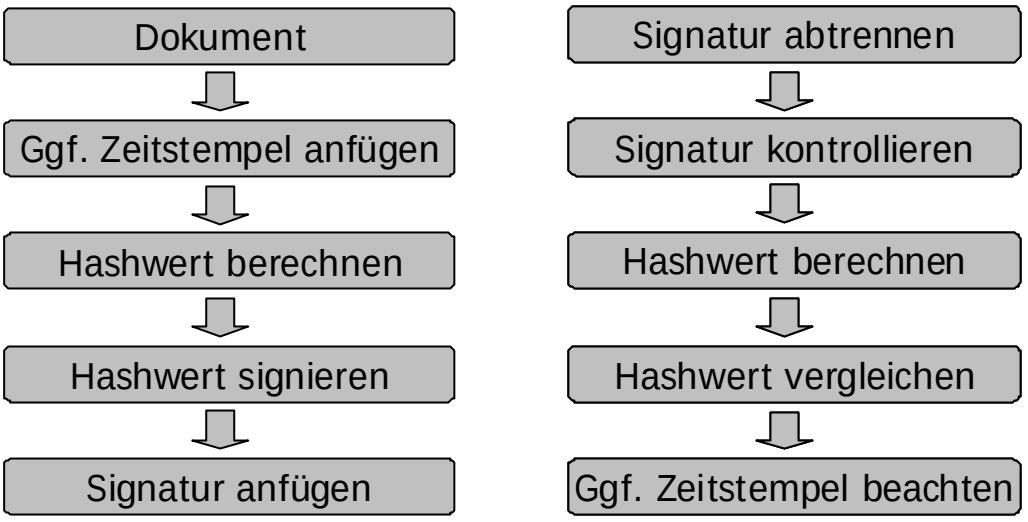

Abbildung 2-6 – Signatur erzeugen und Signatur überprüfen

Quelle: Vergleiche Selke (Kryptographie, 2000), S. 115.

2.2.5 Signaturstrukturen

Obwohl die Funktionsweise der Generierung und Verifizierung klar definiert ist, stehen mehrere unterschiedliche Verfahren zur Verfügung. In dem vorher beschriebenen konventionellen Verfahren wird die Signatur von einem Benutzer erstellt und kann später von jedem beliebigen Nutzer verifiziert werden[98]. Sind an der Generierung und Prüfung einer Signatur mehrere Parteien beteiligt, so werden diese als Multi-Signaturverfahren oder kollektive Signaturverfahren bezeichnet. Weil sowohl bei den konventionellen als auch den Multi-Signaturverfahren immer nur eine Signatur erzeugt und verifiziert wird, werden diese als Mono-Signaturen bezeichnet[99].

Im Gegensatz dazu können zu einem Dokument mehrere separate Signaturen erzeugt werden, an denen wiederum eine oder mehrere Personen beteiligt sind. Hierbei können insbesondere unterschiedliche Signaturverfahren, die auf unterschiedlichen mathematischen Verfahren beruhen, zum Einsatz kommen. Im Idealfall wären zwei mathematische Verfahren zueinander orthogonal, so daß eine Kompromittierung des einen Verfahrens keine Kompromittierung des anderen

[98] Vgl. Schmeh (Kryptographie, 2001), S. 118.

[99] Vgl. Wohlmacher (Digitale Signaturen und Sicherheitsinfrastrukturen, 2001), S. 85

Verfahrens zur Folge hätte. Diese werden als Poly-Signaturen oder multiple Signaturen (Multiple Signatures[100]) bezeichnet, weil in diesem Fall zu einem Dokument immer mehrere Signaturen existieren[101].

Sollen zu einem Dokument mehrere Signaturen erzeugt werden, so können diese auf zwei unterschiedliche Arten generiert werden. Zum einen werden die Signaturen der Reihe nach auf das gleiche Dokument angewendet, so daß diese unabhängig von einander verifiziert werden können. Aus diesem Grund wird von parallelen Signaturen gesprochen. Zum anderen können Signaturen hintereinander auf das Dokument und die vorhergehende Signatur angewendet werden. In diesem Fall müssen die Signaturen alle hintereinander geprüft werden, bevor das Dokument akzeptiert wird. Aus dieser Vorgehensweise leitet sich die Bezeichnung serielle Signaturen ab[102].

Einen Überblick über vorhandene Signaturstrukturen gibt Abbildung 2-7.

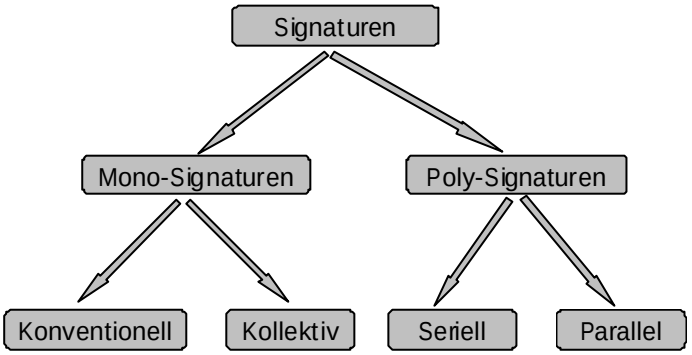

Abbildung 2-7 – Signaturstrukturen im Überblick

Quelle: Wohlmacher (Digitale Signaturen und Sicherheitsinfrastrukturen, 2001), S. 87.

[100] Vgl. Schneier (Applied Cryptography, 1996), S. 39

[101] In der bestehenden Fachliteratur werden Signaturen, an denen mehrere Parteien beteiligt sind, außerdem als Multisignatur, Kollektivsignatur, Mehrfachsignatur oder Gruppensignatur bezeichnet.

[102] Vgl. Wohlmacher (Digitale Signaturen und Sicherheitsinfrastrukturen, 2001), S. 89

2.2.6 Kryptoanalyse

Nachdem Verfahren zur Verschlüsselung und Signatur dargestellt wurden, stellt sich die Frage, ob Sicherheit in dem beschriebenen Maße gewährleistet ist. Um dies einschätzen zu können, werden im folgenden Angriffsmöglichkeiten der Kryptoanalyse[103] beschrieben, denen die Verfahren standhalten müssen.

Alle bisherigen Verfahren zur Sicherung der Anforderungen an die Kommunikation hatten gemeinsam, daß der notwendige Schlüssel nur mit unverhältnismäßig hohem Aufwand ermittelt werden konnte und geheim war. Diese Voraussetzung reicht jedoch nicht aus, um die Sicherheit eines Verfahrens zu gewährleisten. Denn es besteht die Möglichkeit, ohne Kenntnis des geheimen Schlüssels möglichst viele Informationen über den Klartext zu gewinnen[104].

Zunächst geht die Kryptoanalyse davon aus, daß ein Angreifer vollständigen Zugriff auf die elektronisch übertragene Kommunikation hat. Dies ist der ungünstigst anzunehmende Fall, aber es ist klar, daß in jedem anderen Fall das Verfahren nicht unsicherer sein könnte. Von diesem Ansatz aus werden nun vier generelle Angriffsmöglichkeiten unterschieden[105].

Als erstes ist der Geheimtextangriff (ciphertext-only attack) zu nennen. Da diese Methode die schwierigste ist, hilft meist nur der Brute-Force-Angriff, das Durchprobieren sämtlicher möglicher Schlüssel[106]. Sollten Gesetzmäßigkeiten des Geheimtextes bekannt sein, so kann versucht werden, diese auszunutzen. Bei der Caesar-Chiffre wäre dies beispielsweise eine Häufigkeitsanalyse der Buchstaben[107].

Als nächstes wird der Klartextangriff (known-plaintext attack) betrachtet. Hierbei versucht der Angreifer aus dem Geheimtext und einem Teil des Klartextes den

---

[103] Vgl. Schmeh (Kryptographie, 2001), S. 14.

[104] Vgl. Wobst (Abenteuer Kryptologie, 1998), S. 65

[105] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 57;
Vgl. Schneier (Applied Cryptography, 1996), S. 5ff.

[106] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 58;
Vgl. Schmeh (Kryptographie, 2001), S. 75.

[107] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 58.

restlichen Klartext, in der Regel über den Schlüssel, zu gewinnen[108]. Diese wahrscheinlich wichtigste Methode ist wesentlich leistungsfähiger als der Geheimtextangriff, und oft in der Praxis möglich, indem Teile der Nachricht geraten werden. Am Beispiel einer E-Mail kann dies verdeutlicht werden. Zum einen ist der Kopf (Header) der Mail größtenteils bekannt, da er verwendet wird um die Mail zuzustellen[109], zum anderen verwenden viele Personen vordefinierte Textblöcke mit Adresse und Telefonnummer, die an jede Mail angehängt werden und daher bekannt sind[110]. Ein Fehler, der der deutschen Wehrmacht im zweiten Weltkrieg unterlaufen ist, war die verschlüsselte Übertragung öffentlich bekannter Informationen, exemplarisch sei der Wetterbericht erwähnt. Den Kryptoanalytikern stand damit ein langer Klartext zu einem Geheimtext zur Verfügung[111].

Die Chancen des Angreifers werden erhöht, wenn er nicht nur einen Klartext zur Verfügung hat, sondern diesen frei wählen kann (chosen-plaintext attack)[112]. Dies ist in der Praxis jedoch nur möglich, wenn es dem Angreifer gelingt, dem Schlüsselbesitzer den gewünschten Klartext unterzuschieben und ihn anschließend dazu bringt, diesen zu verschlüsseln. Außerdem muß es ihm gelingen, in den Besitz des Geheimtextes zu kommen.

Der letzte Angriff ist eine Abwandlung des vorherigen und nur von theoretischer Bedeutung. Denn ein Angriff mit adaptiv ausgewähltem Klartext (adaptive-chosen-plaintext attack)[113] entspricht einem wiederholt durchgeführten Angriff mit ausgewähltem Klartext, wobei der Klartext jeweils nach dem Resultat des vorher erhaltenen Geheimtextes gewählt werden kann.

---

[108] Vgl. Wobst (Abenteuer Kryptologie, 1998), S. 66

[109] Vgl. Bernstein (Internet mail message header format, 2001), Internet-Quelle;
Vgl. Schneier (Secrets & Lies, 2001), S. 84.

[110] Vgl. Wobst (Abenteuer Kryptologie, 1998), S. 54.

[111] Vgl. Schneier (Secrets & Lies, 2001), S. 84.

[112] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 58;
Vgl. Schneier (Applied Cryptography, 1996), S. 6.

[113] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 58.

Neben diesen generellen Typen gibt es noch weitere, die nicht zu den gebräuchlichen Methoden gehören, aber denkbar sind. Erwähnenswert ist der Angriff mit ausgewähltem Geheimtext (chosen-ciphertext attack)[114], bei dem der Angreifer dem Schlüsselbesitzer den gewünschten Text zum Entschlüsseln vorlegt. Ebenso möglich ist ein Angriff mit verwandten Schlüsseln (chosen key attack)[115], bei dem der Angreifer bekannte Beziehungen zwischen unbekannten Schlüsseln auszunutzen versucht. Daneben gibt es noch den Geheimtext-Geheimtext-Angriff (ciphertext- ciphertext attack)[116], bei dem ein Klartext auf zwei unterschiedliche Methoden chiffriert wird und der Angreifer daraus einen Nutzen zu ziehen versucht, und die gewöhnlichen Verbrechen (rubber-hose attack, purchase-key attack)[117], bei denen der Angreifer durch Erpressung, Entführung, Bestechung oder ähnliches in den Besitz des Schlüssels zu gelangen versucht.

Heutige Kryptosysteme müssen den generellen Typen der Kryptoanalyse der differentiellen Kryptoanalyse[118] und statistischen Auswertungen[119] standhalten. Nach den theoretischen Angriffen sind Implementierungsattacken[120], also Power- und Timingattacken, möglich. Erst wenn ein Algorithmus längere Zeit bekannt ist und von vielen Kryptographen untersucht wurde und keine Schwächen zu Tage getreten sind, ist von seiner Sicherheit auszugehen, sofern er entsprechend implementiert wurde.

Die Geheimhaltung eines Algorithmus stellt auf jeden Fall keine Erhöhung der Sicherheit dar[121], obwohl Angriffe zunächst erschwert werden[122]. Außerdem ist die

---

[114] Vgl. Schneier (Applied Cryptography, 1996), S. 6;
Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 58.

[115] Vgl. Schneier (Applied Cryptography, 1996), S. 7.

[116] Vgl. Wobst (Abenteuer Kryptologie, 1998), S. 66ff

[117] Vgl. Schneier (Applied Cryptography, 1996), S. 7ff

[118] Vgl. Biham/Shamir (Differential cryptanalysis), S. 2ff

[119] Häufigkeitsanalyse von Zeichen innerhalb einer Sprache.

[120] Attacken, die Schwachstellen bei der Implementierung ausnutzen, beispielsweise das Messen von Zeitspannen bei Berechnungen.

[121] Vgl. Schneier (Applied Cryptography, 1996), S. 7f

[122] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 57

tatsächliche Durchführung der Geheimhaltung über lange Zeit zumindest fragwürdig. Als wichtigste Angriffe sind die Rache eines entlassenen Mitarbeiters sowie Erpressung oder Bestechung eines Mitarbeiters zu nennen, die zur Veröffentlichung des Algorithmus führen. In diesem Fall wäre der Schaden, der durch die Weiternutzung eines Algorithmus entsteht, obwohl er nicht mehr sicher ist, wahrscheinlich wesentlich höher. Zudem besteht die Möglichkeit des reverse-engineerings[123] des Algorithmus, so daß kein Produkt vertrieben werden dürfte, in dem der Algorithmus implementiert ist[124].

Es ist festzustellen, daß perfekte Sicherheit[125] nicht zu erreichen ist[126]. Selbst Algorithmen, die jahrelang untersucht und getestet wurden, können durch Fortschritte in der Mathematik[127] oder auf anderen Gebieten[128] unsicher werden. Allerdings ist hier die Wahrscheinlichkeit als gering einzuschätzen und ein Erfolg auf diesem Gebiet wird nicht geheim bleiben, um ausgenutzt werden zu können[129]. Abhilfe schaffen hier nur Verfahren und Protokolle, die nicht auf ein kryptographisches Verfahren festgelegt sind, sondern den Einsatz beliebiger Verfahren erlauben. Ein unsicher gewordenes Verfahren könnte damit leicht durch ein anderes, sicheres Verfahren ausgetauscht werden.

---

[123] Dabei wird das compilierte Programm zurückübersetzt und dadurch der ursprüngliche Quelltext ermittelt.

[124] Vgl. Schneier (Secrets & Lies, 2001), S. 108ff

[125] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 89ff

[126] Ein nach dem Satz von Shannon beweisbar perfektes Kryptosystem ist das Vernam-One-Time-Pad. Es ist das bekannteste, allerdings durch den einmaligen Gebrauch des Schlüssels zu ineffizient, um eingesetzt werden zu können.

[127] Einen solchen Fortschritt könnte beispielsweise ein Algorithmus zur Faktorisierung großer Zahlen darstellen.

[128] Bau des ersten Quantencomputers, der durch die hohe Parallelität sämtliche heute bekannten Public-Key-Verfahren brechen könnte.

[129] Vgl. Buchmann (Faktorisierung großer Zahlen, 2000), S. 6ff.

Das erreichte relative Sicherheitsniveau hängt somit vom eingesetzten Verfahren ab, eine unglückliche Implementierung oder mißratene Protokolle beim Einsatz können dieses Niveau jedoch drastisch senken[130].

2.3 Internetbasierte Kommunikation

Nachdem die Anforderungen der Kommunikation und Grundlagen der Kryptographie erläutert wurden, sollen im folgenden einige der am häufigsten verwendeten Protokolle des Internets näher untersucht werden. Zunächst wird auf Transmission Control Protocol / Internet Protocol (TCP/IP) eingegangen, das ein Basisprotokoll ist, auf dem die später betrachteten Protokolle aufsetzen. Danach werden die Anwendungsprotokolle näher betrachtet, die von 95%[131] der Internet-User verwendet werden. Dabei handelt es sich zum einen um das HyperText Transfer Protocol (HTTP) zur Übertragung von Webseiten sowie um das Simple Mail Transfer Protocol (SMTP) zum Versenden und das Post Office Protocol Version 3 (POP3) zum Abholen der Mails. Das mächtigere Internet Message Access Protocol, Version 4 (IMAP4)[132] wird aufgrund der wesentlich geringeren Verbreitung nicht betrachtet[133].

2.3.1 TCP/IP

Ende der sechziger Jahre begann die Entwicklung von TCP/IP durch das US-Verteidigungsministerium (Department of Defense)[134] mit dem Ziel einer weiträumigen Vernetzung von Großrechnern. Ein Forschungsbereich des Ministeriums, die Advanced Research Projects Agency (ARPA), sollte nach Technologien suchen, die dem Militär von Vorteil sein könnten. 1969 entstand das verbindungsorientierte ARPANET, mit einem eigens dafür entwickelten, paketvermittelten

---

[130] Vgl. Schneier (Secrets & Lies, 2001), S. x.

[131] Vgl. Merz (Electronic Commerce, 1999), S. 39.

[132] Vgl. Crispin (IMAP4 - RFC 1730, 1994), Internet-Quelle.

[133] Vgl. Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 385

[134] Vgl. Smith (Internet Kryptographie, 1998), S. 29.

Übertragungsverfahren, das militärisch und von einigen großen amerikanischen Universitäten genutzt wurde[135]. Eine wichtige im Entwurf spezifizierte Eigenschaft sah vor, daß ein Knoten des Netzes jeweils mit mindestens zwei anderen Knoten verbunden sein sollte. Insbesondere sollte es für eine Nachricht möglich sein, auf mehreren Wegen zum Ziel zu gelangen. Da eine Nachricht in Pakete aufgeteilt wird, wenn ihre Länge eine definierte Grenze[136] übersteigt, können sogar einzelne Teile einer Nachricht unterschiedliche Wege benutzen. Durch diesen dezentralen Aufbau ist die Funktionsfähigkeit des Netzes gewährleistet, selbst wenn Teile der Infrastruktur zerstört sind[137]. Aus diesem Vorteil resultiert jedoch, daß ein Nutzer in der Regel keinen Einfluß[138] auf den Weg eines Paketes hat und die Nachricht viele andere Rechner passiert, die sie zum Beispiel lesen oder manipulieren könnten.

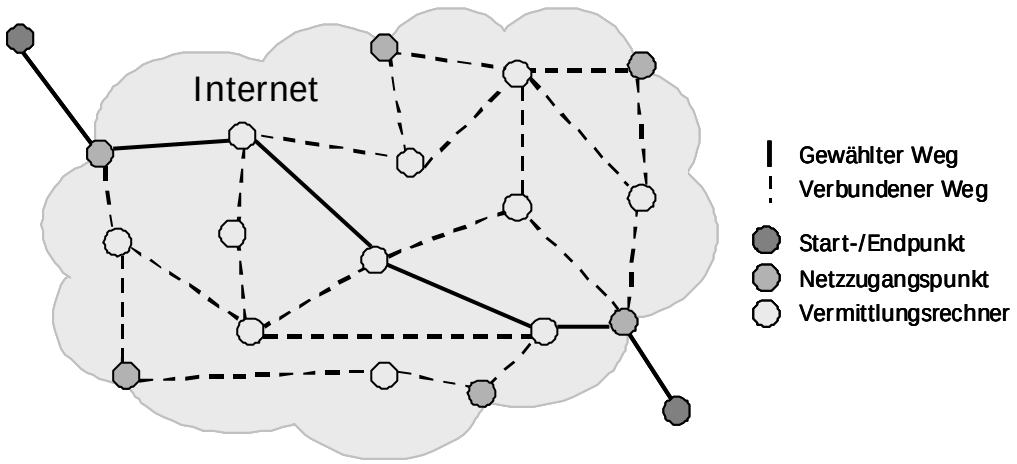

Abbildung 2-8 – Darstellung eines Nachrichtenweges im Internet

[135] Vgl. Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 40.

[136] 1536 Bytes abzüglich der Steuerungsinformationen für das Paket.

[137] Zu beachten ist, daß aus Kostengründen Knotenpunkte in Frankfurt, London oder New York entstanden sind, die diesem Gedanken eigentlich widersprechen, da ein Ausfall von der restlichen Infrastruktur nicht abgefangen werden könnte. Vgl. Höge (Im Datenknast, 2001), S. 66, 68.

[138] Eine Angriffsmöglichkeit besteht damit in der Veränderung dieser Routenwahl.

Die Protokolle TCP[139] und IP[140] entstanden aus einer Weiterentwicklung aus dem Jahre 1973, die zum Ziel hatte, heterogene paketvermittelte Netze zu verbinden. 1983 erfolgte zum einen die Trennung des ARPANET in das militärisch genutzte MILNET sowie das privat genutzte ARPANET[141], zum anderen die Umstellung auf TCP/IP, das für Unix entwickelt wurde und zugleich einfach und zuverlässig sein sollte[142].

In dem 1977 verabschiedeten Open Systems Interconnection-Referenzmodell (OSI-Referenzmodell)[143] von der International Standardization Organisation (ISO) sollten Regeln für die Funktionsweise der Kommunikation in heterogenen Systemen festgelegt werden[144]. Dabei kann TCP der Transportschicht, Schicht 4, und IP der Vermittlungsschicht, Schicht 3, zugerechnet werden. Darunter, in den Schichten 1 und 2, befinden sich die Protokolle, die für die physische Übertragung der Daten zuständig sind. Beide Protokolle verfügen über keinerlei Sicherungsmöglichkeiten, abgesehen von der in jedem Rahmen übermittelten Prüfzahl zur Fehlererkennung[145]. Dies muß von den darüberliegenden Schichten, der Sitzungs-, Darstellungs- und Anwendungsschicht, übernommen werden. Eine Darstellung des ISO/OSI-Referenzmodells findet sich in Abbildung 2-9.

---

[139] Vgl. Postel (TCP - RFC 793, 1981), Internet-Quelle.

[140] Vgl. Postel (IP - RFC 791, 1981), Internet-Quelle.

[141] Vgl. Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 40.

[142] Vgl. Tanenbaum, Computer-Netzwerke, S. 717

[143] Vgl. Eckert (IT-Sicherheit, 2001), S. 41.

[144] Vgl. Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 27;
Vgl. Tanenbaum (Moderne Betriebssysteme, 1995), S. 486ff.

[145] Diese findet in der der Sicherungsschicht (Schicht 2) statt. Siehe Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 33.

Abbildung 2-9 – ISO/OSI-Referenzmodell

Quelle: Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 27

2.3.2 Electronic Mail

Electronic Mail, unter anderem mit den Protokollen SMTP[146] und POP3[147] realisiert, setzt auf TCP auf und ist den Schichten 5-7 des ISO/OSI-Referenzmodells zuzurechnen. Dies sind die Sitzungsschicht, die für die Steuerung und Synchronisation der Nachrichtenübertragung verantwortlich ist, die Darstellungsschicht, die die semantische Interpretation der empfangenen Daten vornimmt und die Anwendungsschicht, die dem User die gewünschte Funktionalität innerhalb einer Oberfläche zur Verfügung stellt.

Ursprünglich bestand eine Mail nur aus reinem Text, sogenannten American National Standard Code for Information Interchange Zeichen (ASCII-Zeichen)[148]. Um Bilder, Audio- oder Videodaten versenden zu können, wurde 1992 von der Inter-

[146] Vgl. Postel (SMTP - RFC 821, 1982), Internet-Quelle.

[147] Vgl. Rose (POP3 - RFC 1081, 1988), Internet-Quelle.

[148] Vgl. American National Standards Institute (ASCII, 1997), Internet-Quelle.

net Engineering Task Force (IETF) das Multipurpose Internet Mail Extensions Format (MIME-Format) für Mails eingeführt[149].

Beim Versand einer elektronischen Mail wird diese über das SMTP-Protokoll an einen SMTP-Server versendet und von dort an den Server des Empfängers weitergeleitet, der die Nachricht in das entsprechende Postfach ablegt. Dort kann sie der Empfänger mittels des POP3-Protokolls abholen. Zusammen mit TCP/IP sind diese Protokolle nicht geeignet, alle Anforderungen an die Kommunikation zu erfüllen. Denn die Nachricht kann auf jedem Rechner, den sie passiert, gelesen und manipuliert werden. Zudem gibt es keine Überprüfung, ob der in der Mail eingetragene Absender der tatsächliche Absender ist[150]. Als letzte sicherheitsrelevante Tatsache soll erwähnt werden, daß das Paßwort zum Abholen der Mails im Klartext übertragen wird, so daß ein Abhören möglich ist[151].

2.3.3 HTTP

Beim Hypertext-Transferprotokoll handelt es sich wie bei Elektronic Mail um ein auf TCP aufsetzendes Protokoll[152], das samt des für die Darstellung nötigen Browsers ebenfalls den Schichten 5-7 des ISO/OSI-Referenzmodells zuzurechnen

---

[149] Vgl. Freed/Borenstein (MIME (1) - RFC 2045, 1996), Internet-Quelle;
Vgl. Freed/Borenstein (MIME (2) - RFC 2046, 1996), Internet-Quelle;
Vgl. Moore (MIME (3) - RFC 2047, 1996), Internet-Quelle;
Vgl. Freed/Klensin/Postel (MIME (4) - RFC 2048, 1996), Internet-Quelle;
Vgl. Freed/Borenstein (MIME (5) - RFC 2049, 1996), Internet-Quelle;
Vgl. Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 386.

[150] Dies ermöglichte die massenweise unerwünscht versendeten Werbemails, bekannt unter dem Namen SPAM. Zur Eindämmung wurden SMTP-Server umkonfiguriert, so daß nur noch Mails bestimmter Absender versandt werden konnten. Mittlerweise setzt sich immer mehr das Verfahren POP-before-SMTP durch, bei dem erst Mails abgeholt werden müssen, bevor andere versandt werden können. Die Authentifizierung beim Abholen der Mails wird damit für den Versand von Mails benutzt.

[151] Vgl. Bitzer/Brisch (Digitale Signatur, 1999), S. 3.

[152] Vgl. Smith (Internet Kryptographie, 1998), S. 244.

ist[153]. Ein wesentliches Merkmal des Protokolls ist die Zustandslosigkeit[154], die bedeutet, daß die aufgebaute Verbindung nach jeder Anfrage des Clients und Antwort des Servers wieder abgebaut wird. Eine Verbindung läuft dabei wie in Abbildung 2-10 zu sehen ab. Zunächst wird die Verbindung aufgebaut. Daraufhin übermittelt der Client die Anfrage an den Server, die dieser beantwortet. Nach dem Erhalt der Nachricht durch den Client wird die Verbindung wieder abgebaut.

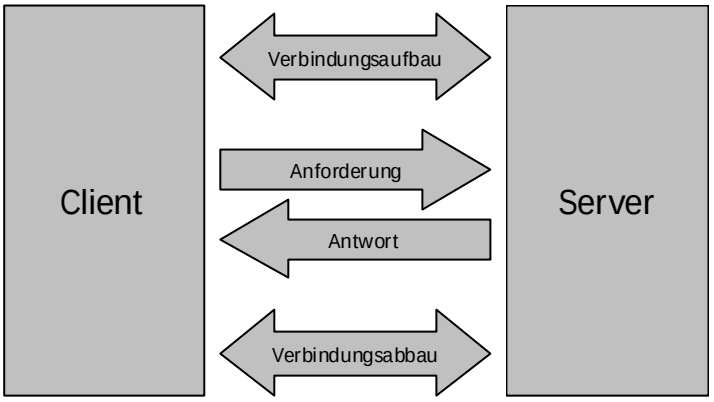

Abbildung 2-10 – Ablauf des Hypertext-Transferprotokolls
Quelle: Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 370.

In der ersten Version des Protokolls (HTTP/0.9) war nur die Möglichkeit eines Simple Request mittels einer einfachen GET-Anweisung gegeben[155]. Dieser geringe Funktionsumfang war ausreichend, da zu Beginn des World Wide Web (WWW) nur statische Seiten übertragen wurden. Mit der Zunahme der dynamischen Seiten und der damit zusammenhängenden Erhöhung der Anforderungen einer Anfrage an einen Server wurde in der Version 1.0 der Full Request eingeführt[156]. Die

[153] Dabei ist das Hypertext-Transferprotokoll nur der Sitzungs- und Darstellungsschicht zuzurechnen. Der Web-Browser, der für die Anzeige der Daten zuständig ist, implementiert das Protokoll und damit die Anwendungsschicht, so daß insgesamt von den Schichten 5-7 zu sprechen ist.

[154] Vgl. Eckert (IT-Sicherheit, 2001), S. 71.

[155] Vgl. Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 371.

[156] Vgl. Berners-Lee/Fielding/Frystyk (HTTP/1.0 - RFC 1945, 1996), Internet-Quelle.

Weiterentwicklung zur Version 1.1[157] mit der Einführung der Host Header wurde schließlich notwendig, um eine vollständige Trennung zwischen dem Domain-Namen und der IP-Adresse zu erreichen. Es wurde somit möglich, mehrere Domains auf einer IP-Adresse zu betreiben und trotzdem über unterschiedliche Webserver für die Domains zu verfügen[158].

Zu erwähnen ist, daß mit den Erweiterungen des Protokolls die Zustandslosigkeit teilweise behoben wurde. Bei mehrstufigen Transaktionen konnten somit Folgen von Objekten ohne Unterbrechung der Verbindung übertragen werden. Insbesondere beim Laden einer HyperText Markup Language-Seite (HTML-Seite)[159] müssen somit für die Bilder der Seite keine neuen Verbindungen geöffnet werden. Bei hintereinander ausgeführten Transaktionen besteht die Zustandslosigkeit jedoch nach wie vor[160].

Dieser Nachteil kann durch Cookies behoben werden, die Sessioninformationen auf dem Client speichern und diese bei jedem erneuten Zugriff zum Server übertragen. Diese Cookies speichern zwar den Namen des Servers, können aber trotzdem, je nach Einstellung, von anderen Servern gelesen werden[161]. Daraus ergibt sich, daß Cookies mit gebotener Vorsicht zu behandeln sind, da sie zum einen datenschutzrechtlichen Bestimmungen zuwider laufen können und zum anderen durch den Zugriff auf den Rechner des Clients ein Gefahrenpotential darstellen.

Eine weitere Möglichkeit, den Nachteil der Zustandslosigkeit zu beheben, ist die Übertragung einer Session-ID bei jeder Anfrage. Durch diese ID können die Informationen der Session auf dem Server gespeichert und trotzdem dem Client zu-

---

[157] Vgl. Fielding/Gettys/Frystyk/Berners-Lee (HTTP/1.1 - RFC 2068, 1997), Internet-Quelle; Vgl. FieldingGettys/Mogul/Frystyk/Masinter/Leach/Berners-Lee (HTTP/1.1 - RFC 2616, 1999), Internet-Quelle.

[158] Vgl. FieldingGettys/Mogul/Frystyk/Masinter/Leach/Berners-Lee (HTTP/1.1 - RFC 2616, 1999), Kapitel 5.2.1.

[159] Vgl. Berners-Lee/Connolly, D. (HTML - RFC 1866, 1995), Internet-Quelle.

[160] Vgl. Smith (Internet Kryptographie, 1998), S. 244.

[161] Vgl. Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 371.

geordnet werden. Diese weit verbreitete Art wird beispielsweise von Suchmaschinen und Webshops[162] eingesetzt.

Einige moderne Anwendungen des Internet, wie zum Beispiel die Banking-Applikationen der Direktbanken, erfordern jedoch weitergehende Sicherheitsmaßnahmen. Dabei sind die weiter oben genannten Anforderungen an die elektronische Kommunikation, für die das Protokoll nicht ausgelegt ist, entscheidend für die Akzeptanz der Anwendung.

2.3.4 Kryptographische Protokolle

Um Authentizität, Integrität, Vertraulichkeit und Verbindlichkeit garantieren zu können, müssen demnach kryptographische Protokolle eingesetzt werden.

Hier ist zunächst Secure/MIME (S/MIME)[163] für elektronische Mails zu nennen, das in der Version 3 aus dem Jahre 1999 stammt. In dieser Erweiterung des MIME-Formats ist es möglich, den Inhalt einer Mail verschlüsselt zu versenden oder zusätzliche Daten zur Authentifizierung des Absenders anzuhängen. Da es sich bei dieser Erweiterung nur um zusätzliche Typen handelt, mußte das eigentliche Protokoll nicht geändert werden.

Um das HTTP-Protokoll abzusichern, gibt es mehrere Ersatzprotokolle, von denen zuerst das Secure Hypertext Transfer Protocol (S-HTTP)[164] als Erweiterung von HTTP genannt werden soll[165]. Obwohl es sich hierbei um einen Standard der IETF handelt, konnte es sich aufgrund der schwierigen Konfiguration und den in den HTML-Dokumenten durchzuführenden Sicherheitsmaßnahmen nicht durchsetzen. Außerdem ist S-HTTP als Erweiterung von HTTP auf WWW-Anwendungen beschränkt.

Während S-HTTP dazu gedacht ist, sichere Nachrichten über das Internet zu verschicken, erstellt Secure Sockets Layer (SSL), von Netscape 1994 veröffentlicht,

---

[162] Ein Beispiel hierfür ist Amazon, unter www.amazon.de.

[163] Vgl. Ramsdell (S/MIME - RFC 2633, 1999), Internet-Quelle;
Version 2 in RFC 2311 bis 2315.

[164] Vgl. Rescorla/Schiffman (S-HTTP - RFC 2660, 1999), Internet-Quelle.

[165] Vgl. Häckelmann/Petzold/Strahringer (Kommunikationssysteme, 2000), S. 372.

eine sichere Ende-zu-Ende-Verbindung vom Client zum Server[166]. Das Protokoll selbst besteht wiederum aus 2 Protokollen. Zum einen dem SSL Record Protocol, das höhere Protokolle einschließt, und zum anderen dem SSL Handshake Protocol, das die Authentifizierung von Client und Server durchführt und zum Aushandeln[167] der kryptographischen Verfahren sowie Austauschen der Schlüssel verwendet wird. Ein großer Vorteil ist die Unabhängigkeit von anderen Protokollen, so daß SSL neben HTTP auch andere Dienste wie SMTP, FTP oder Telnet absichern kann.

2.4 Austausch von Schlüsseln mit Zertifikaten

Nachdem die kryptographischen Grundlagen und die Protokollen zum Nachrichtenaustausch im Internet erläutert wurden, wird deutlich, daß bis auf Verbindlichkeit sämtliche Anforderungen an die Kommunikation erfüllt werden können. Während weder E-Mail noch HTTP den Empfang einer Nachricht bestätigen können, kann Vertraulichkeit durch Verschlüsselung gewährleistet werden. Die Integrität einer Nachricht kann mit Hilfe eines signierten Hashwertes erreicht werden. Gleichzeitig bestätigt diese Signatur, daß die Nachricht mit einem bestimmten, zum öffentlichen passenden, privaten Schlüssel verschlüsselt wurde.
Da ein öffentlicher Schlüssel alleine nicht die Identität einer Person bestätigt, wird ein zusätzliches Instrument, ein sogenanntes Zertifikat[168], zur Authentifizierung benötigt. Im folgenden werden der Aufbau und Einsatz solcher Zertifikate beschrieben, bevor Methoden zur Wiederherstellung von Schlüsseln untersucht werden.

---

[166] Vgl. Selke (Kryptographie, 2000), S. 190;
Vgl. o.V. (Webopedia, 2001), SSL.

[167] Aushandeln bedeutet in diesem Fall, daß die Liste der bekannten Verfahren von Client und Server nach einem Verfahren durchsucht wird, welches von beiden unterstützt wird. Weiterhin hat es zur Folge, daß leicht auf ein neues Verfahren umgestiegen werden kann, da nicht alle Rechner zur gleichen Zeit umgestellt werden müssen.

[168] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 210.

2.4.1 Aufbau eines Zertifikates

Die meist verwendeten Zertifikate sind Zertifikate nach dem X.509-Standard[169], der einer der wichtigsten Kryptostandards überhaupt ist[170]. Ursprünglich nur als Authentifizierungsstandard für den Verzeichnisdienst X.500 geplant, ist die Nutzung im Internet im Grunde ein Mißbrauch. Die erste, 1988 erschienene Version X.509v1, verfügt über 7 Felder, die in Abbildung 2-11 abgebildet sind.

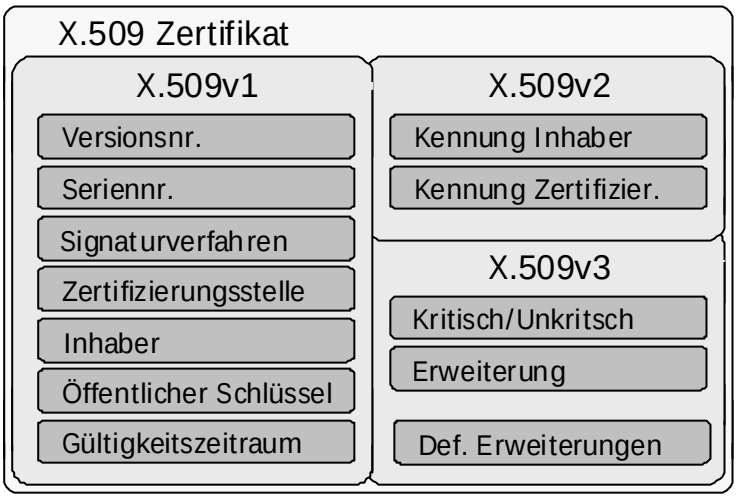

Abbildung 2-11 – Aufbau eines X.509-Zertifikates

Diese Felder enthalten die mindestens notwendigen Daten, über die ein Zertifikat verfügen muß[171]. Es stellte sich rasch heraus, daß diese in den meisten Fällen nicht ausreichend waren. Eine zweite Version, X.509v2 die 2 Felder hinzufügte[172], wurde daher 1993 veröffentlicht Es sind dies zum einen eine eindeutige Kennung des Zertifikatsinhabers, zum anderen eine der Zertifizierungsinstanz. Bedeutung kam die-

---

[169] Vgl. Chadwick/Basden (Evaluation Trust in a Public Key Certification Authority, 2001), S. 592.

[170] Vgl. Schmeh (Kryptographie, 2001), S. 323;
Vgl. Schneier (Applied Cryptography, 1996), S. 575.

[171] Vgl. Hastenteufel/Meinel (Digitale Zertifikate - Standards und Anwendungen, 1999), S. 9;
Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 5;
RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 15.

ser Version nicht zu, da diese Felder bis heute kaum genutzt werden und die benötigten Felder weiterhin fehlten, exemplarisch seien Altersbegrenzung oder monetäre Grenzen genannt[173].

1996 kam es zu einer dritten Version des X.509-Standards[174], die einige Probleme beseitigte, aber neue Schwierigkeiten schuf. X.509v3 sah keine neuen Felder vor, sondern spezifizierte eine Syntax, mit der neue Felder hinzugefügt werden können. Dabei wird über ein zusätzliches Attribut festgelegt, ob es sich um eine kritische oder unkritische Erweiterung handelt[175]. Eine Software, die eine kritische Erweiterung nicht kennt, muß daher das gesamte Zertifikat als ungültig betrachten, während sie eine unkritische übergehen kann. Dies hat den Vorteil, daß es keine fehlenden Felder mehr gibt. Andererseits bedeutet diese Offenheit der Erweiterbarkeit, daß ein X.509v3-Zertfikat nicht automatisch für alle Anwendungen lesbar ist, die X.509v3-Zertifikate unterstützen[176]. 1997 wurde X.509v3 durch sogenannte Amendments erweitert, um einem Wildwuchs im Bereich der Zertifikatserweiterungen vorzubeugen. Die spezifizierten Erweiterungen, die fester Bestandteil des X.509v3-Standards sind, wurden mit der festgelegten Erweiterungssyntax definiert. Beispiele für diese Erweiterungen sind der Verwendungszweck des Schlüssels, ein zusätzlicher Name des Zertifikatsbesitzers[177] oder Sperrlisten-Verteilungspunkte.

Public-Key-Infrastructure X.509 (PKIX)[178] und die Industrial Signature Interoperability Specification (ISIS)[179] beschreiben nicht nur, wie diese Erweiterungen verwendet werden sollen, sondern definieren ebenfalls eigene Erweiterungen. Wäh-

---

[172] Vgl. Eckert (IT-Sicherheit, 2001), S. 266.

[173] Vgl. Schmeh (Kryptographie, 2001), S. 314.

[174] Vgl. Eckert (IT-Sicherheit, 2001), S. 266.

[175] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 84.

[176] Vgl. Schmeh (Kryptographie, 2001), S. 316f.

[177] Dieser muß nicht mehr ein X.500-Name sein. Möglich ist beispielsweise eine EMail-Adresse.

[178] Vgl. PKIX Working Group (Webseite der PKIX Working Group, 2001), Internet-Quelle.

[179] Vgl. T7 Organisation (Webseite der T7 Organisation, 2001), Internet-Quelle.

rend sich PKIX mit dem Informationszugang zur Zertifizierungsstelle[180] (Certification Authority, CA) begnügt, definiert ISIS für das deutsche Signaturgesetz relevante Erweiterungen. Als wichtigste seien Nutzungsbeschränkungen, Vertretungsbefugnisse, monetäre Beschränkungen oder Volljährigkeit genannt[181].

Für einige der in den Erweiterungen genutzten Informationen kann es sinnvoll sein, sie in einer eigenen Datenstruktur auszulagern, die einem Zertifikat ähnelt, aber keinen öffentlichen Schlüssel enthält. Zur Abgrenzung gegenüber einem Zertifikat, das in diesem Zusammenhang ebenso Schlüsselzertifikat genannt werden kann, wird diese Struktur Attribut-Zertifikat genannt[182]. Ein Anwendungsfall wäre zum Beispiel die Speicherung auf einer Chipkarte, die nur begrenzten Speicher platz zur Verfügung stellt[183]. Ebenso ist die Gültigkeit eines Attribut-Zertifikates unabhängig von der des Schlüssel-Zertifikates und ein Attribut-Zertifikat kann unter Verschluß gehalten werden, was aus Sicht des Datenschutzes sinnvoll sein kann.

2.4.2 Einsatz von Zertifikaten

Mit Hilfe eines Zertifikates ist die Zuordnung eines öffentlichen Schlüssels zu einer Person möglich, wobei das Zertifikat an sich ebenfalls signiert werden muß[184]. Die Signatur garantiert die überprüfbare Integrität des Zertifikates, implizit bedeutet dies jedoch, daß dem Aussteller der Signatur vertraut werden muß.

Bei diesem Aussteller des Zertifikates handelt es sich um einen vertrauenswürdigen Dritten[185]. Bevor der Sender einem unbekannten Kommunikationspartner eine

---

[180] Nach dem Signaturgesetz korrekt Zertifizierungsdiensteanbieter.

[181] Vgl. Blum (Entwurf eines neuen Signaturgesetzes, 2001), S. 72.

[182] Vgl. Schmeh (Kryptographie, 2001), S. 321;
Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 84;
Vgl. Hastenteufel/Meinel (Digitale Zertifikate - Standards und Anwendungen, 1999), S. 8.

[183] Vgl. Schmeh (Kryptographie, 2001), S. 321.

[184] Vgl. Dusemund/Becker/Gollan/Engel/Meinel (The Functionality of a Public Key Infrastructure, 2000), S. 9.

[185] Vgl. Schneier (Secrets & Lies, 2001), S. 217

verschlüsselte Mail zukommen lassen kann, besorgt er sich von einem vertrauenswürdigen Dritten ein Zertifikat, das den Namen an den öffentlichen Schlüssel bindet. Mit diesem kann er die Nachricht verschlüsseln und signieren und sie dem Empfänger zukommen lassen. Der Empfänger wiederum holt sich das Zertifikat des Senders und verifiziert mit diesem die Signatur. Aus diesem Grund muß eine Struktur existieren, die es erlaubt, Zertifikate zweifelsfrei zu erhalten und zu kontrollieren. Ansonsten könnte ein Angreifer dem Sender und Empfänger jeweils ein Zertifikat mit seinem öffentlichen Schlüssel unterschieben und so die Kommunikation abhören oder sogar fälschen[186].

Diese Struktur wird von einer Zertifizierungsstelle[187] zur Verfügung gestellt[188]. Es wird jedoch deutlich, daß sich beim Verlust eines privaten Schlüssels ein Dritter mit Hilfe des Zertifikates der Identität des gefundenen Schlüssels bemächtigen kann. Deshalb müssen Verfahren existieren, um ein Zertifikat innerhalb des Gültigkeitszeitraums widerrufen zu können.

Wurden wichtige Daten mit dem eigenen öffentlichen Schlüssel aus Sicherheitsgründen verschlüsselt, so wären diese ebenfalls vom Verlust eines privaten Schlüssels betroffen, da dem Besitzer wie jedem Angreifer nur das vollständige Durchsuchen des Schlüsselraumes zur Wiederherstellung der Daten bliebe.

Während dies bei einer Privatperson noch als eigenverschuldetes Unglück betrachtet werden könnte, sieht die Situation für ein Unternehmen anders aus. Hier könnte ein gekündigter Mitarbeiter böswillig seinen Schlüssel vernichten, was für das Unternehmen einen Datenverlust aller nicht mehr unverschlüsselt vorliegender Daten zur Folge hätte[189].

---

[186] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 209.

[187] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 88.

[188] Sämtliche Dienste werden in Kapitel 4 betrachtet.

[189] Zumindest bis durch schnellere Rechner und viel Zeit die Schlüssel wiedergewonnen worden wären.

2.4.3 Wiederherstellung von Schlüsseln

Da die Verfahren ausgelegt sind, um eine Wiederherstellung des Schlüssels aus dem öffentlichen Schlüssel zu verhindern, muß ein anderer Weg genutzt werden. Eine Möglichkeit sind geänderte Verschlüsselungsprozesse, beispielsweise die zusätzliche Verschlüsselung für einen vertrauenswürdigen Dritten (Trusted Third-party Encryption)[190], der Arbeitgeber des Mitarbeiters[191]. In diesem Fall verschlüsselt der Client des Benutzers die Nachricht oder die Datei nicht nur mit dem eigenen öffentlichen Schlüssel oder dem des Empfängers, sondern zusätzlich - und ohne die Möglichkeit, dies zu unterbinden - mit dem Schlüssel des Unternehmens, bei dem der Benutzer angestellt ist. Dies geschieht sogar ohne daß der Benutzer etwas davon merkt und somit erhält das Unternehmen Zugriff auf jegliche Kommunikation beziehungsweise Daten[192].

In diesem Zusammenhang wird oft die Notwendigkeit einer Regierung angeführt, aus sicherheitspolitischen Gründen jegliche Kommunikation abhören zu wollen, um Verbrechen aufdecken zu können[193]. Da sich jedoch beispielsweise ein Terrorist nicht an bestehende Gesetze halten wird, wenn er einen Terroranschlag plant, wird er eine doppelte Verschlüsselung für die Regierung auf jeden Fall vermeiden. Daher ist die Motivation für den Regierungszugriff auf Schlüssel höchst zweifelhaft[194].

Die Verschlüsselung für einen vertrauenswürdigen Dritten hat im Ergebnis einen sehr sensitiven geheimen Schlüssel. Im Falle der Kompromittierung dieses Schlüssels wäre nicht nur die Kommunikation eines Mitarbeiters, sondern die aller Mit-

---

[190] Vgl. Zimmermann (Message from Phil Zimmermann, Creator of PGP, 2000), Internet-Quelle.

[191] Vgl. Schneier (Secrets & Lies, 2001), S. 234;
Vgl. Key Recovery Alliance (Technology Papers, Special Issue - Introduction, 2000), S. 19.

[192] Vgl. Eckert (IT-Sicherheit, 2001), S. 296.

[193] Vgl. Langenbach/Ulrich (Elektronische Signaturen, 2002), S. 24;
Vgl. Schneier (Secrets & Lies, 2001), S. 233.

[194] Vgl. Anderson/Diffie/Neumann/Rivest/Schneier and more (The risks of key recovery, 2001), Internet-Quelle;
Vgl. Schneier (Secrets & Lies, 2001), S. 235.

arbeiter - beziehungsweise sogar aller Menschen, die diese Software nutzen - aufgedeckt. Diejenigen Mitarbeiter der Regierung, die mit solchen Schlüsseln umgehen, wären ideale Angriffspunkte für Angreifer jeder Art[195].

2.5 Mitarbeiterzertifikate

Aus diesem Grund sollte jeder private Schlüssel nur genau einmal gespeichert sein, und zwar im Hoheitsbereich des Benutzers. Idealerweise geschieht dies auf einer Smartcard, aus der der Schlüssel nicht ausgelesen werden kann. Statt dessen werden die Daten zur Karte übertragen, dort mit dem privaten Schlüssel ent- beziehungsweise verschlüsselt und wieder zurückübertragen.

Verfügen Mitarbeiter eines Unternehmens über Smartcards, die sie in Ihrer Tätigkeit als Mitarbeiter verwenden, so hat das Unternehmen in manchen Fällen Interesse an der Smartcard eines Mitarbeiters, zum Beispiel beim Ausscheiden des Mitarbeiters aus dem Unternehmen. Dies bedeutet für den Mitarbeiter ein enormes Druckmittel, da er mit dem mutwilligen Verlust oder der Zerstörung der Karte Daten des Unternehmen vernichtet[196].

Die Zertifizierungsstelle könnte vom Unternehmen aufgefordert werden, eine Kopie des Schlüssels geschützt aufzubewahren[197], jedoch hätte dies eine zentrale Hinterlegung aller Schlüssel mit den daraus resultierenden Sicherheitsbedenken zur Folge.

Eine Möglichkeit, diesem Mißbrauch vorzubeugen, wäre, dem Unternehmen eine Kopie der Smartcard des Mitarbeiters zu übergeben. Dies wäre für das Unternehmen ausreichend, da es damit jederzeit vollständigen Zugriff auf alle Daten der Mitarbeiter hätte. Andererseits birgt diese Vorgehensweise ein großes Risiko, denn dieser Zugriff könnte von den Mitarbeitern des Unternehmens, die Zugriff auf die-

---

[195] Vgl. Ross (PGP: Backdoors and Key Escrow, 2001), Internet-Quelle;
Vgl. Wiesner (Key Recovery, 2000), S. 703.

[196] Vgl. Schmeh (Kryptographie, 2001), S. 305;
Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 35.

[197] Vgl. Bitzer/Brisch (Digitale Signatur, 1999), S. 34.

se Smartcards haben, mißbraucht werden[198]. Da die Karten allerdings sehr sicher aufbewahrt werden müssen, ist eine Lösung denkbar, bei der mindestens zwei oder mehr hochrangige Mitarbeiter des Unternehmens gleichzeitig anwesend sein müssen, um Zugang zu den Smartcards zu erhalten. Weiterhin attraktiv wäre dieser Ort jedoch für Angreifer, da sie mit einem Einbruch an sämtliche Schlüssel des Unternehmens gelangen könnten.

Die geschilderten Probleme ließen sich durch eine spezielle Mitarbeiter-Smartcard umgehen. Zum einen erhielte der Mitarbeiter eine normale Smartcard, zum anderen würde jedoch immer eine zweite Karte ausgestellt, auf der sich ebenfalls der private Schlüssel des Mitarbeiters befindet. Dieser muß jedoch erstens durch den Schlüssel der Zertifizierungsstelle geschützt, beziehungsweise verschlüsselt sein, zweitens kann diese Karte nicht direkt zum Ver- oder Entschlüsseln verwendet werden. Diese Karte erhält das Unternehmen, bei dem der Mitarbeiter angestellt ist. Das Unternehmen kann zunächst nichts mit der Karte anfangen, da der Schlüssel des Mitarbeiters durch den der Zertifizierungsstelle geschützt ist. Im Falle des Verlustes einer Mitarbeiterkarte kann das Unternehmen, gegebenenfalls durch eine notarielle Bestätigung, ein Duplikat der Karte des Mitarbeiters herstellen. Dabei wird das Zertifikat des Mitarbeiters ungültig, damit jeglicher Mißbrauch von Seiten des Unternehmens ausgeschlossen wird, aber verschlüsselte Daten nicht verloren gehen.

2.6 Zertifizierungsstellen

Damit Sender und Empfänger zweifelsfrei miteinander kommunizieren können und dabei keine Angriffe von Dritten befürchten müssen, brauchen sie nach den obigen Erläuterungen Zertifikate, die von einer Zertifizierungsstelle[199] ausgegeben werden,

---

[198] Der Schlüssel könnte zusätzlich in mehrere Teile zerlegt werden. Weitere Verfahren siehe Wiesner (Key Recovery, 2000), S. 699ff.

[199] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 34;
Vgl. ebenda, S. 88;
Vgl. Schmeh (Kryptographie, 2001), S. 284.

die als vertrauenswürdiger Dritter fungiert. Diese bürgt mit ihrer Signatur für die ausgegebenen Zertifikate, das heißt für Korrektheit und Gültigkeit[200] der öffentlichen Schlüssel der Teilnehmer[201].

In den folgenden Kapiteln sollen zunächst die notwendigen Funktionen[202] einer Zertifizierungsstelle vorgestellt werden, bevor zum Abschluß auf Zertifikatsketten eingegangen wird.

2.6.1 Funktionen einer Zertifizierungsstelle

Um Zertifikate verwenden zu können, muß jeder neue Benutzer zunächst registriert werden. Dazu ist eine Authentifizierung der Zertifizierungsstelle notwendig[203]. Der Benutzer muß entweder persönlich erscheinen und sich mit einem Ausweis legitimieren oder auf andere Verfahren - wie beispielsweise Post-Ident[204] - zurückgreifen. Der Benutzer bekommt einen persönlichen Namen zugewiesen, unter dem er Signaturen erzeugen kann. Jedoch ist es ebenfalls möglich, anstelle des richtigen Namens ein Pseudonym zu verwenden. In diesem Fall sind die Identität und weitere persönliche Daten nur der Zertifizierungsstelle bekannt.

Eine weitere Funktion ist die Schlüsselerzeugung, wenn der Benutzer nicht einen selbsterzeugten Schlüssel zertifizieren lassen möchte. Die Zertifizierungsstelle speichert den erzeugten Schlüssel im sichersten Fall direkt auf einer Chipkarte, von der dieser Schlüssel nicht ausgelesen werden kann. Der Benutzer kann in diesem Fall den Schlüssel auch nicht unwissentlich verraten, da er ihn nicht kennt[205].

Mit dem Schlüssel erstellt die Zertifizierungsstelle ein Zertifikat, in dem unter anderem der Name oder das Pseudonym, der zugeordnete Schlüssel, der Name der

---

[200] Die Gültigkeit hat zumindest bis zur eventuellen Sperrung des Zertifikates durch den Teilnehmer bestand.

[201] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 209ff

[202] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 49;
Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 4.

[203] Vgl. Eckert (IT-Sicherheit, 2001), S. 265.

[204] Hierbei handelt es sich um ein Verfahren zur Authentifizierung in einer Post-Filiale.

[205] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 210

Zertifizierungsstelle und die Gültigkeit vermerkt sind[206]. Dieses wird in ein Verzeichnis[207] eingetragen, in das nur die Zertifizierungsstelle schreiben kann. Lesender Zugriff wird jedoch für alle Benutzer gewährt, damit die Zertifikate verwendet werden können[208].

Sämtliche öffentliche Schlüssel müssen außerdem archiviert werden, wobei die Dauer der Aufbewahrung von der Verwendung des Schlüssels abhängt. Mit Hilfe der Archivierung kann die Gültigkeit eines Schlüssels nachgewiesen werden, wenn nach Ablauf eines Zertifikates dessen Gültigkeit zum Nachweis benötigt wird[209].

Da die Gültigkeit eines Zertifikates beschränkt ist, muß es rechtzeitig vor Ablauf ausgetauscht werden. Dabei muß der neue Schlüssel jedoch so zum Benutzer gelangen, daß er sicher bleibt, selbst wenn der ablaufende Schlüssel kompromittiert wird. Eine Verschlüsselung des neuen privaten Schlüssels mit dem alten öffentlichen ist demnach keine Lösung[210].

In manchen Fällen, zum Beispiel bei Verlust des privaten Schlüssels, muß ein Zertifikat vor Ablauf der Gültigkeit ungültig gemacht werden. Für diese Fälle gibt es bei der Zertifizierungsstelle eine Liste der ungültigen Zertifikate (CRL, Certificate Revocation List). Diese ist Teil des Verzeichnisses und muß bei jeder Prüfung eines Zertifikates überprüft werden, bevor die Gültigkeit festgestellt werden kann[211].

Als eine weitere Funktion einer Zertifizierungsstelle sei die Herausgabe eines ungültigen archivierten Schlüssels genannt, wobei der Benutzer gegebenenfalls seine Berechtigung zum Erhalt des Schlüssels nachweisen muß.

---

[206] Vgl. Kapitel 2.4.1.

[207] Vgl. Falk/Trommer (Nutzung von Verzeichnisdiensten, 1999), S. 97.

[208] Vgl. Harnier (Organisationsmöglichkeiten für Zertifizierungsstellen, 2000), S. 79;
Vgl. Schmeh (Kryptographie, 2001), S. 327ff.

[209] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 210;
Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 5.

[210] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 212.

[211] Vgl. Schmeh (Kryptographie, 2001), S. 337.

Als letztes soll die Funktion eines Zeitstempels[212] erwähnt werden, den eine Zertifizierungsstelle anbieten kann, aber nicht muß. Dieser Dienst ist jedoch für die Ausstellung von Zertifikaten notwendig, damit zum Beispiel der Zeitpunkt der Erstellung oder Löschung exakt dokumentiert ist. Ebenso ist der Zeitpunkt der Erstellung der CRL von Bedeutung. Benutzer können den Zeitstempeldienst ebenfalls benötigen, wenn der Zeitpunkt der Nachrichtensendung von Bedeutung ist, wie es beispielsweise beim Kauf von Aktien oder einer notariellen Beurkundung der Fall ist[213].

2.6.2 Zertifikatsketten

Weiter oben wurde beschrieben, daß eine Zertifizierungsstelle ein Verzeichnis aller gültigen Zertifikate führt. Der Sender einer Nachricht muß daher bei seiner Zertifizierungsstelle den Schlüssel des Empfängers erfragen. Im einfachen Fall hat diese das Zertifikat selbst ausgestellt. Da ihm der öffentliche Schlüssel der Zertifizierungsstelle bekannt ist, kann er die Signatur überprüfen und den öffentlichen Schlüssel verwenden[214].

Andernfalls muß der Sender das Zertifikat indirekt erhalten. Zuerst muß er herausfinden, welche Zertifizierungsstelle das Zertifikat des Empfängers ausgestellt hat. Verfügt seine Zertifizierungsstelle über ein Zertifikat der Zertifizierungsstelle des Empfängers, so kann er deren öffentlichen Schlüssel bereits überprüfen. Mit diesem Schlüssel kann er dann die Echtheit des Zertifikates verifizieren, um schließlich in Kontakt mit dem Empfänger zu treten. Verfügt seine Zertifizierungsstelle über kein Zertifikat der anderen Zertifizierungsstelle, so muß der Sender einen Weg, eine Zertifikatskette[215], von seiner zu der des Empfängers finden, um das Zertifikat überprüfen zu können.

---

[212] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 38.

[213] Vgl. Kühn (Technische Grundlagen, 1999), S. 86.

[214] Vgl. Horster/Kraaibeek/Wohlmacher (Sicherheitsinfrastrukturen - Basiskonzepte, 1999), S. 10, 12.

[215] Vgl. Baum (Gültigkeitsmodell des SigG, 1999), S. 200.

Dabei ist wichtig, daß keine Zertifizierungsstelle innerhalb der Kette vorkommt, der der Sender nicht vertraut. Außerdem setzt dieses Verfahren Transitivität voraus[216], das heißt wenn Zertifizierungsstelle Z_1 auf Z_2 vertraut und Z_2 auf Z_3, dann vertraut Z_1 auch Z_3[217].

[216] Vgl. Purser (A Simple Graphical Tool For Modelling Trust, 2001), S. 480.

[217] Am Beispiel eines Baumes vgl. Schneier (Applied Cryptography, 1996), S. 576.

3 Rechtliche Grundlagen und organisatorische Konsequenzen

Nachdem die technischen Grundlagen einer Public-Key-Infrastruktur in Kapitel zwei betrachtet wurden und deren Eignung für den Einsatz der Erfüllung der Anforderungen an die Kommunikation bestätigt wurde, folgt in diesem Kapitel die Beschreibung der rechtlichen Situation in Deutschland. Begonnen wird mit einer Beschreibung der betreffenden Regelungen, anschließend werden die daraus resultierenden organisatorischen Konsequenzen abgeleitet.

3.1 Zertifizierungsstellen betreffende Regelungen

Als Mitglied der europäischen Union gilt für Deutschland, wie für jedes andere Mitgliedsland: Vorrangige europarechtliche Normen gilt es im deutschen Recht zu beachten, Richtlinienvorgaben entsprechend in deutsches Recht umzusetzen. Aus diesem Grund ist es nicht ausreichend, nur die nationalen Gesetze zu betrachten[218].

Als erstes wird die europäische Signaturrichtlinie vorgestellt, im Anschluß daran folgt eine Darstellung des deutschen Signaturgesetzes. Nicht betrachtet wird das Formanpassungsgesetz[219], welches die digitale Signatur an einzelnen Stellen in das BGB integriert und damit die Nutzung ermöglicht. Detailliertere Ausführungen wurden aus diesem Gesetz in die Signaturverordnung ausgelagert, die im dritten Abschnitt erläutert wird. Um beim Aufbau eines Zertifizierungsdiensteanbieters den Anforderungen des Gesetzgebers entsprechen zu können, wird zum Abschluß

---

[218] Vgl. Schmeh (Kryptographie, 2001), S. 470ff

[219] BGBl. I 2001 Nr. 35, S. 1544ff.

Das vollständige Gesetz ist im Anhang abgedruckt.

das IT-Grundschutzhandbuch (IT-GSHB)[220] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschrieben, weil es die technischen Lücken der vorher erwähnten Regelungen schließt[221]. Die Reihenfolge der Betrachtung wird in Abbildung 3-1 dargestellt.

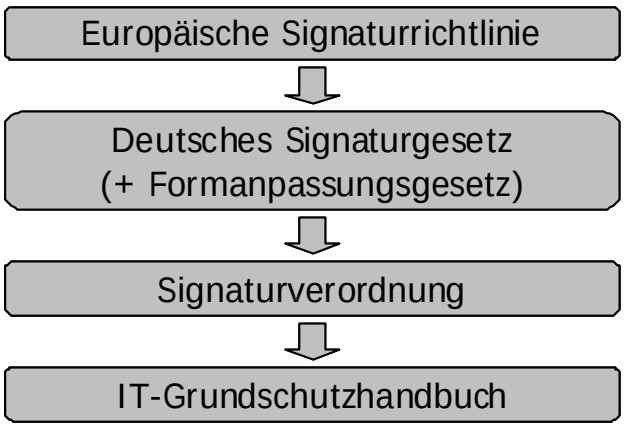

Abbildung 3-1 – Reihenfolge der gesetzlichen Regelungen

3.1.1 Europäische Signaturrichtlinie

Weder durch die Richtlinie 1999/93/EG des Europäischen Parlaments und des Europäischen Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, der europäischen Signaturrichtlinie[222], noch durch in der Folgezeit zur Regelung der gemeinschaftsrechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr von den zuständigen Organen der europäischen Union erlassene sogenannte E-Commerce Richtlinie (Richtlinie 2000/31/EG, Abl. EG 2000 Nr. L178, S. 1ff), werden detaillierte Angaben zu elektronischen Signaturen gemacht. Vielmehr werden für bestimmte rechtliche

---

[220] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Internet-Quelle.

[221] Das Datenschutzgesetz wurde aufgrund der dadurch entstehenden Komplexität nicht in die Betrachtungen der Arbeit einbezogen. Im Anhang der Arbeit befinden sich die Richtlinie 1999/93/EG der Europäischen Union, das Signaturgesetz sowie die Signaturverordnung.

[222] RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13.Dezember 1999. Abl. EG 2000 Nr. L13, S. 12.

Aspekte der Dienste einer Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt Rahmenbedingungen geschaffen[223].

In Artikel 1 der europäischen Signaturrichtlinie wird der Anwendungsbereich der Richtlinie festgelegt, der die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen soll. Für Zertifizierungsdienste werden Rahmenbedingungen spezifiziert. Ausdrücklich werden weder der Abschluß noch die Gültigkeit von Verträgen erwähnt, da hier nach einzelstaatlichem Recht oder Gemeinschaftsrecht Formvorschriften zu erfüllen sind. In den Begriffsbestimmungen in Artikel 2 werden Ausdrücke der Richtlinie erläutert, angefangen bei der ‚elektronischen Signatur' über ‚Zertifikate' und ‚qualifizierte Zertifikate' bis hin zur ‚freiwilligen Akkreditierung'.

In Artikel 3 wird der Marktzugang festgelegt, der nicht von einer vorherigen Genehmigung abhängig zu machen ist (Absatz 1). Freiwillige Akkreditierungssysteme zur Steigerung des Sicherheitsniveaus können eingeführt beziehungsweise beibehalten werden, wobei die Anforderungen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein müssen. Eine Überwachung der Zertifizierungsdiensteanbieter, die öffentlich qualifizierte Zertifikate ausstellen, muß von den Mitgliedsstaaten eingerichtet werden. Mitgliedsstaaten haben zusätzlich die Möglichkeit, Signaturen im öffentlichen Bereich weiteren Anforderungen zu unterwerfen (Absatz 7).

Die Rechtswirkung elektronischer Signaturen wird in Artikel 5 geregelt. Dieser legt fest, daß eine Unterschrift in elektronischer Form die Anforderungen an eine Unterschrift in gleicher Weise wie die handschriftliche Unterschrift erfüllt und in Gerichten als Beweismittel zuzulassen ist, sofern sie mit einer fortgeschrittenen elektronischen Signatur, die auf einem qualifizierten Zertifikat beruht, erstellt wurde. Die rechtliche Wirksamkeit darf einer elektronischen Signatur nicht abgesprochen werden, nur weil diese Anforderungen nicht erfüllt sind.

Artikel 6 legt die Haftung von Zertifizierungsdiensteanbietern fest, sofern dieser nicht nachweisen kann, daß er nicht fahrlässig gehandelt hat. Die Haftung bezieht

---

[223] Vgl. Roßnagel (Elektronische Signaturen in Europa, 1998), S. 331.

sich beispielsweise auf alle Informationen in dem qualifizierten Zertifikat (Absatz 1) oder einen nicht registrierten Widerruf des Zertifikates (Absatz 2).
Artikel 7 legt fest, daß qualifizierte Zertifikate eines Mitgliedsstaates denen anderer Staaten gleichgestellt werden, um grenzüberschreitende Zertifizierungsdienste zu erleichtern. Artikel 8 bestimmt, daß die Regelungen des Datenschutzes der Richtlinie 95/46/EG eingehalten werden müssen[224]. In Artikel 12 wird festgelegt, daß die Kommission die Durchführung der Richtlinie überprüft und spätestens zum 19.07.2003 darüber Bericht erstattet.
In den Anhängen der Richtlinie werden die Anforderungen an qualifizierte Zertifikate (Anhang I), an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen (Anhang II), an sichere Signaturerstellungseinheiten (Anhang III) sowie Empfehlungen für die sichere Signaturprüfung (Anhang IV) spezifiziert.

3.1.2 Signaturgesetz

Bereits vor der europäischen Signaturrichtlinie hatte Deutschland am 1. August 1997 das Signaturgesetz (SigG) als Teil des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) verabschiedet. Dieses sehr strenge Gesetz[225] legte bereits in seiner ursprünglichen Fassung[226] einen hohen Sicherheitsstandard für elektronische Signaturen fest, um insbesondere die Betreiber von Zertifizierungsstellen zu Sicherheitsmaßnahmen zu animieren[227]. Da die europäische Richtlinie diesen Vorgaben nicht folgte, wurde am 21. Mai 2001 das neue Signaturgesetz erlassen[228].

---

[224] Aufgrund der entstehenden Komplexität werden diese Aspekte in der Arbeit jedoch vernachlässigt.

[225] Diese Einschätzung wird weiter unten im Absatz Anbieterakkreditierung spezifiziert. Siehe auch Gollan/Meinel (Electronic Signatures, 2000), S. 15.

[226] Beachte aber die heutige Fassung vom 16.05.2001. SigG, BGBl. I 2001, S. 876ff.

[227] Vgl. Schmeh (Kryptographie, 2001), S. 472

[228] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001. Vgl. BGBl. Jahrgang 2001 Teil I Nr. 22, S. 876ff.

In den allgemeinen Bestimmungen des Gesetzes, dem ersten Abschnitt, werden elektronische Signaturen als elektronische Daten angesehen, die in einer beliebigen Form den Daten beigefügt, beziehungsweise logisch mit ihnen verknüpft sind.

> *§2 Nr. 1. [Im Sinne dieses Gesetzes sind] "elektronische Signaturen" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.*

Erst eine fortgeschrittene elektronische Signatur ist dem Schlüsselinhaber zugeordnet und entspricht dem intuitiven Verständnis einer Signatur[229]. Das Sicherheitsniveau wird durch eine qualifizierte elektronische Signatur gesteigert, die zusätzlich auf einem qualifizierten Zertifikat beruhen muß[230].
Zertifikate werden als elektronische Bescheinigungen definiert, mit denen ein Signaturschlüssel einer Person zugeordnet und dabei die Identität dieser Person bestätigt wird (§2 Nr. 6 SigG). Qualifizierte Zertifikate verfügen über einen höheren Sicherheitsstandard, da mindestens die Voraussetzungen von SigG §§4ff. oder §23 und §24 in Verbindung mit der SigV[231] erfüllt sein müssen[232].
Im zweiten Abschnitt des Gesetzes werden die Anforderungen an den Zertifizierungsdiensteanbieter erläutert. Nach der Feststellung, daß der Betrieb einer Zertifizierungsstelle im Rahmen der Gesetze genehmigungsfrei ist[233], werden die notwendigen Voraussetzungen näher erläutert. Dabei wird in Absatz 3 eine Anzeigepflicht erwähnt, die jedoch nicht im Signaturgesetz, sondern in der Signaturverordnung spezifiziert wird. Bei der Vergabe der qualifizierten Zertifikate wird die Verfügbarkeit der Dienste sowie die Möglichkeit der Nutzung eines Pseudonyms beschrieben. Des weiteren wird die Unterrichtungspflicht des Zertifizierungsdien-

---

[229] Im gesamten Dokument ist mit einer digitalen Signatur immer eine fortgeschrittene elektronische Signatur gemeint.

[230] Vgl. Roßnagel (Das neue Signaturgesetz, 2001), S. 202.

[231] Signaturverordnung vom 16.05.2001, BGBl. I 2001, S. 3074ff.

[232] Darüber hinaus besteht die Möglichkeit der freiwilligen Akkreditierung nach §15, die die vermutete Sicherheit in behördlich überprüfte Sicherheit überführt.

[233] Vgl. SigG, §4 (1).

steanbieters gegenüber den Teilnehmern, bei der sie über die Möglichkeiten und Risiken aufgeklärt werden müssen, und der Inhalt qualifizierter Zertifikate genannt. Neben der Sperrung von qualifizierten Zertifikaten werden qualifizierte Zeitstempel erwähnt. Den Abschluß bilden Paragraphen über die Dokumentation (§10), Haftung (§11), Deckungsvorsorge (§12) sowie den Datenschutz (§14). Die gesetzlich geforderte Vorhaltung einer geeigneten Deckungsvorsorge soll den Regreß gegen Zertifizierungsstellen bei Pflichtwidrigkeit sichern helfen; diese darf den Betrag von 250.000 € pro haftungsauslösendem Ereignis nicht unterschreiten. (Mindestsumme gemäß §12 Satz 2 SigG in Verbindung mit Artikel 2 Nr. 1, BGBl. I 2001, S. 883)

Im dritten Abschnitt, der freiwilligen Akkreditierung, werden die Modalitäten derselben definiert. Darüber hinaus erhält der öffentliche Bereich die Möglichkeit, diese per Rechtsvorschrift zu verlangen. Akkreditierte Zertifizierungsdiensteanbieter erhalten von der zuständigen Behörde ein Zertifikat, welches sie als solche ausweist.

Im vierten Abschnitt wird auf die technische Sicherheit eingegangen, wobei sich dies auf Produkte und die Anerkennung von Prüf- und Bestätigungsstellen bezieht. Aufsichtsmaßnahmen und Mitwirkungspflichten werden darauf folgend erläutert.

Im sechsten Abschnitt, den Schlußbestimmungen, werden Bußgeldvorschriften sowie Kosten und Beiträge für Amtshandlungen dargelegt. Ebenso wird die Behandlung ausländischer elektronischer Signaturen beziehungsweise Produkte geregelt.

3.1.3 Signaturverordnung

Das Signaturgesetz verwendet an einigen Stellen Begriffe, die nicht genau spezifiziert werden. Diese Lücken werden von der Signaturverordnung geschlossen[234]. Beispielsweise spricht das Signaturgesetz in §4 (3) von einer Anzeige in geeigneter

[234] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001. Vgl. BGBl. Jahrgang 2001 Teil I Nr. 59, S. 3074ff.

Form; die formalen Anforderungen werden in der Signaturverordnung §1 erläutert.

In §1 werden neben der Form auch der Inhalt und die Änderung einer Anzeige der Betriebsaufnahme einer Zertifizierungsstelle beziehungsweise eines Zertifizierungsdienstes spezifiziert.

> *§1 (1) Eine Anzeige nach § 4 Abs. 3 des Signaturgesetzes ist schriftlich oder mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen bei der zuständigen Behörde vorzunehmen.*
> *(2) Die Anzeige muss folgende Angaben und Unterlagen umfassen:*
> *1. den Namen und die Anschrift des Zertifizierungsdiensteanbieters,*
> *2. die Namen der gesetzlichen Vertreter,*
> *3. aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für den Zertifizierungsdiensteanbieter und seine gesetzlichen Vertreter,*
> *4. einen aktuellen Handelsregisterauszug oder eine vergleichbare Unterlage,*
> *5. Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde nach § 4 Abs. 2 Satz 3 des Signaturgesetzes,*
> *6. ein Sicherheitskonzept mit einer genauen Darlegung, wie dieses umgesetzt ist, einschließlich der Übertragung von Aufgaben an Dritte nach § 4 Abs. 5 des Signaturgesetzes, und*
> *7. einen Nachweis der Deckungsvorsorge nach § 12 des Signaturgesetzes.*
> *Ändern sich die Umstände nach Satz 1 Nr. 1 oder Nr. 2 oder sicherheitserhebliche Umstände nach Satz 1 Nr. 6, ist die zuständige Behörde schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu informieren. § 2 bleibt unberührt.*

In §2 wird der notwendige Inhalt eines Sicherheitskonzeptes beschrieben, das im Signaturgesetz[235] und in §1 der Signaturverordnung genannt wird. Erwähnung finden hierbei nicht nur technische, bauliche und organisatorische Sicherheitsmaßnahmen, sondern darüber hinaus eingesetzte Produkte, die Aufbau- und Ablaufor-

[235] Vgl. SigG §4 Abs. 2 Satz 4.

ganisation, Notfallmaßnahmen, Auswahl des Personals und eine Abschätzung und Bewertung verbleibender Sicherheitsrisiken. Namentlich muß darin enthalten sein:

> *§2 Das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 des Signaturgesetzes hat Folgendes zu enthalten:*
> *1. eine Beschreibung aller erforderlichen technischen, baulichen und organisatorischen Sicherheitsmaßnahmen und deren Eignung,*
> *2. eine Übersicht über die eingesetzten Produkte für qualifizierte elektronische Signaturen mit Herstellererklärungen nach § 17 Abs. 4 Satz 2 oder Bestätigungen nach § 17 Abs. 4 Satz 1 oder nach § 15 Abs. 7 Satz 1 des Signaturgesetzes,*
> *3. eine Übersicht über die Aufbau- und Ablauforganisation sowie die Zertifizierungstätigkeit,*
> *4. die Vorkehrungen und Maßnahmen zur Sicherstellung und Aufrechterhaltung des Betriebes, insbesondere bei Notfällen,*
> *5. die Verfahren zur Beurteilung und Sicherstellung der Zuverlässigkeit des eingesetzten Personals und*
> *6. eine Abschätzung und Bewertung verbleibender Sicherheitsrisiken.*

Um die Identitätsprüfung und Attributsnachweise geht es in §3 der SigV. Es wird festgelegt, daß die Identifizierung anhand des Bundespersonalausweises, des Reisepasses oder anhand von Dokumenten mit gleichwertiger Sicherheit (§3 I S. 1 SigV.) erfolgen muß. Ebenso reicht die Signierung des Antrages für ein qualifiziertes Zertifikat, wenn diese mit einem qualifizierten Zertifikat durchgeführt wird. Daher kann beim Ablauf eines Zertifikates der Erhalt des neuen per Signatur bestätigt werden und damit der Prozeß vollständig elektronisch abgewickelt werden.
Im Anschluß daran wird die Führung eines Zertifikatsverzeichnisses, insbesondere die Aufbewahrungspflichten, spezifiziert. Es folgen einzelne Sicherheitsvorkehrungen des Zertifizierungsdiensteanbieters (§5), beispielsweise betreffend die Signaturerstellungseinheit, sowie die Ausgestaltung der Unterrichtung (§6).
Bezüglich des Verfahrens zur Sperrung von Zertifikaten wird lediglich verlangt, daß eine Rufnummer zur Verfügung stehen soll, unter der Berechtigte ihr Zertifi-

kat sperren können[236]. Der Nachweis ihrer Identität ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen (§7 II Satz 1 SigV).

In §8 wird in Ausführung des §10 SigG der Umfang der Dokumentationspflicht festgelegt. Weiter regelt die Signaturverordnung Details zur Ausgestaltung der Deckungsvorsorge (§9 SigV; §12 SigG) und die freiwillige Akkreditierung und deren Ablauf (§11 SigV; §15 SigG). In §12 und §13 werden die Festsetzung und Erhebung von Kosten und Beiträgen spezifiziert. Ebenso werden in der Signaturverordnung Anforderungen an Inhalt und Gültigkeitsdauer von qualifizierten Zertifikaten und an Produkte für elektronische Signaturen geregelt. Hier ist hervorzuheben, daß ein Signaturschlüssel erst nach Identifikation des Benutzers durch Besitz und Wissen oder Besitz und biometrisches Merkmal angewendet werden kann, wobei er dabei von der Anwendung nicht preisgegeben werden darf (§15 I Satz 1+2 SigV). Es wird hinzugefügt, daß weder aus dem Signaturprüfschlüssel noch aus der Signatur die Signaturschlüssel ermittelt werden können dürfen und daß dies gewährleistet werden muß. Des weiteren darf eine Sperrung nicht unbemerkt rückgängig gemacht werden. Weiter werden in diesem Paragraphen Kriterien zur Evaluierung der Sicherheit der Komponenten spezifiziert, die entweder nach den Common Criteria (CC) for International Electrotechnical Commission (IEC) oder den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) zertifiziert werden müssen.

§17 regelt Verfahren zur langfristigen Speicherung von Daten, die insbesondere von Bedeutung sind, weil kein bekanntes Verfahren für mehr als 5 Jahre als sicher angesehen wird. Danach werden noch zusätzliche Anforderungen an den öffentlichen Bereich definiert, bevor abschließend Verfahren zur Feststellung der gleichwertigen Sicherheit von ausländischen elektronischen Signaturen und Produkten hinsichtlich § 23 des Signaturgesetzes spezifiziert werden.

---

[236] SigV §7. Siehe dazu auch Blum (Entwurf eines neuen Signaturgesetzes, 2001), S. 73.

3.1.4 Grundschutzhandbuch des BSI

Die Signaturverordnung gamäß §4 Abs. 2 Satz 4 des Signaturgesetzes nennt in §2 Nr. 1 Inhalte des Sicherheitskonzeptes.

> *§2 Nr. 1. eine Beschreibung aller erforderlichen technischen, baulichen und organisatorischen Sicherheitsmaßnahmen und deren Eignung,*

Anhaltspunkte hierfür liefert das GSHB des BSI[237]. In diesem wird im Gegensatz zur traditionellen Erstellung eines Sicherheitskonzeptes mit Hilfe einer Risikoanalyse ein Soll-Ist-Vergleich zwischen empfohlenen und bereits realisierten Maßnahmen durchgeführt[238]. Wird für einzelne Komponenten hoher oder sehr hoher Schutzbedarf festgestellt, so ist eine ergänzende IT-Sicherheitsanalyse durchzuführen[239], wie in Abbildung 3-2 dargestellt.

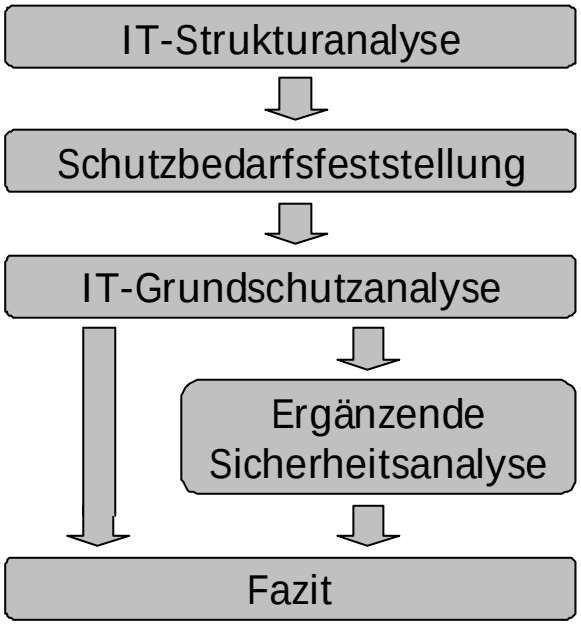

Abbildung 3-2 - Erstellung eines IT-Sicherheitskonzeptes
Quelle: BSI (IT-Grundschutzhandbuch, 2001), Kapitel 2.

[237] Vgl. Ermächtigung hierfür im SigG §24, Rechtsverordnung.

[238] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 1.1.

[239] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 2.

Das Grundschutzhandbuch ist in Bausteine aufgeteilt, die verschiedene Komponenten darstellen. Beispiele hierfür sind die Infrastruktur oder die Telekommunikation. Für jeden dieser Bausteine existieren fünf Gefährdungskataloge, angefangen bei höherer Gewalt über organisatorische Mängel, menschliche Fehlhandlungen und technisches Versagen bis hin zu vorsätzlichen Handlungen. Für jede in den Gefährdungskatalogen genannten Gefährdungen sind Maßnahmen zu ergreifen, die in Maßnahmenkatalogen gruppiert sind. Diese reichen von infrastrukturellen über personelle bis hin zu Notfallvorsorge-Maßnahmen. Aufgrund in der Realität herrschender Ressourcenknappheit können nicht alle Maßnahmen zur gleichen Zeit realisiert werden, weshalb jeder Maßnahme eine von drei Prioritätsstufen zugewiesen wird[240].

Für den Betrieb eines Zertifizierungsdiensteanbieters sind fast alle im Grundschutzhandbuch genannten Bausteine relevant. In den übergeordneten Komponenten sind dies unter anderem Organisation, Personal, Datenschutz, Virenschutz, Kryptoschutz[241]. Im Baustein Infrastruktur werden als wichtigste das Gebäude, die Verkabelung oder die Räume genannt, die wiederum in Büroraum, Serverraum, Datenträgerarchiv und Raum für technische Infrastruktur unterschieden werden. Es folgen Bausteine über vernetzte und nicht vernetzte Systeme, wobei nach Betriebssystemen und Art der Vernetzung unterschieden wird. Datenübertragungseinrichtungen, die mit zunehmender Vernetzung an Bedeutung gewinnen, werden unter anderem nach Datenträgeraustausch, Firewall[242], E-Mail, Webserver und entfernte Zugriffe unterschieden. Den Abschluß bilden Telekommunikations- und sonstige IT-Komponenten, angefangen bei der Telekommunikations-Anlage (TK-Anlage) über das Mobiltelefon bis hin zu Standardsoftware[243].

---

[240] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 1.2.

[241] Die restlichen Komponenten sind das IT-Sicherheitskonzept, das Notfallvorsorgekonzept, das Datensicherungskonzept, die Behandlung von Sicherheitsvorfällen und das Hard- und Softwaremanagement.

[242] Vgl. Schneier (Secrets & Lies, 2001), S. 181.

[243] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 1.4.

Wenn ein Zertifizierungsdiensteanbieter den Nachweis der Sicherheit erbringen will, so bietet das Grundschutzhandbuch dafür eine geeignete Grundlage, weil die genannten Maßnahmen überprüfbar installiert werden können. Durch die Einführung des IT-Grundschutz-Zertifikates durch das BSI im Juli 2001 wird dem Sachverhalt Rechnung getragen, daß dieser Nachweis immer häufiger geführt werden muß[244].

3.2 Organisatorische Konsequenzen

Nachdem im vorherigen Abschnitt die Gesetzeslage für signaturgesetzkonforme Zertifizierungsstellen dargestellt wurde, sollen in diesem Abschnitt die daraus resultierenden Funktionalitäten und die dafür benötigte Infrastruktur beschrieben werden.

3.2.1 Funktionalitäten von Zertifizierungsstellen

Durch die Europäische Signaturrichtlinie, das Signaturgesetz, die Signaturverordnung und das IT-Grundschutzhandbuch des BSI werden Funktionalitäten im Rahmen des organisatorischen Ablaufs beim Betrieb einer Zertifizierungsstelle vorgesehen, damit die Anforderungen an die digitalen Signaturen erfüllt werden[245]. Aus diesen Funktionalitäten wiederum resultieren die zu erbringenden Dienstleistungen, die im wesentlichen die Erzeugung und Vergabe von Schlüsselpaaren samt Zertifizierung zu genau identifizierbaren Personen sowie nachvollziehbare Dokumentation beinhalten[246].

In folgender Abbildung 3-3 sind die Funktionalitäten einer Zertifizierungsstelle abgebildet. Während fünf aufeinanderfolgende Funktionalitäten den Prozeß der Ausstellung eines Zertifikates repräsentieren und demnach pro ausgestelltem Zertifikat einmal durchgeführt werden müssen, ist die Sperrung eines Zertifikates

---

[244] Vgl. BSI (IT-Grundschutz-Zertifikat, 2001), Internet-Quelle.

[245] Nach Gritzalis/Katsikas/Lekkas/Moulinos/Polydorou (The KEYSTROKE PKI Architecture, 2001), S. 736 sind diese allgemeingültig.

[246] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 5.

durch das Sperrmanagement optional. Im Gegensatz dazu können der Verzeichnis- und Zeitstempeldienst, die zur Überprüfung von Zertifikaten und Zeitstempeln vorgesehen sind, pro Zertifikat mehrmals genutzt werden. Die restlichen Funktionalitäten richten sich nicht nach der Anzahl der Zertifikate, sondern nach zeitlichen Vorgaben. Beispielsweise muß eine Datensicherung täglich vorgenommen werden.

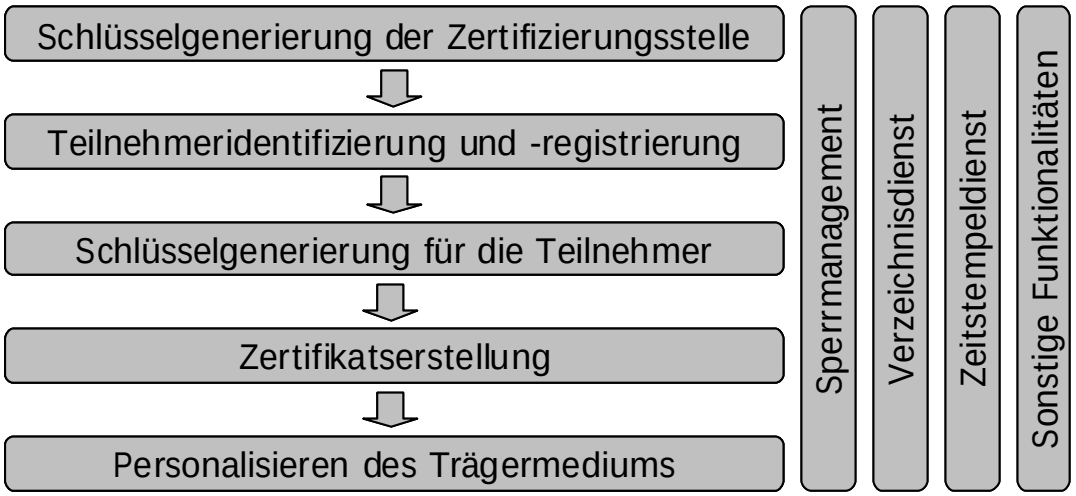

Abbildung 3-3 – Funktionalitäten einer Zertifizierungsstelle

Schlüsselgenerierung der Zertifizierungsstelle

Bevor die Zertifizierungsstelle ihren Dienst aufnehmen kann, muß sie für sich selbst ein eigenes Schlüsselpaar, bestehend aus dem privaten und öffentlichen Schlüssel, erzeugen[247]. Die Schlüssellänge kann, bis auf die in den Richtlinien des

[247] Vgl. Camphausen/Kelm/Liedke/Weber (Aufbau und Betrieb einer Zertifizierungsinstanz, 2001), S. 47;
Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 6.
Aus Sicherheitsgründen sollten zwei unterschiedliche Schlüssel für Zertifikate und Zeitstempeldienstleistungen erzeugt werden, da Zeitstempel häufiger als Zertifikate ausgestellt werden und die vorhandene Anzahl an chiffrierten Daten die Kryptoanalyse vereinfacht. Vgl. hierzu Kapitel 2.2.6.
Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 70.

BSI[248] angegebenen für das gewählte Verfahren mindestens notwendigen Länge, frei gewählt werden. Ein längerer Schlüssel erhöht zwar die Sicherheit, jedoch ebenfalls die zur Verifizierung benötigte Rechenzeit. Da dem Schlüssel einer Zertifizierungsstelle große Bedeutung zukommt, sollte die Entscheidung zugunsten der Sicherheit und damit einer möglichst großen Schlüssellänge ausfallen[249].
Die Schlüsselgenerierung muß innerhalb der Zertifizierungsstelle in einer geeigneten und sicheren Umgebung stattfinden[250]. Weiterhin muß sichergestellt werden, daß ein unautorisierter Zugriff auf den privaten Schlüssel verhindert wird.
Befindet sich die Zertifizierungsstelle innerhalb einer Hierarchie, beispielsweise wie im Signaturgesetz vorgesehen unterhalb der Wurzelinstanz der Zertifizierungsstelle der Regulierungsbehörde, muß das erzeugte Schlüsselpaar, beziehungsweise der öffentliche Schlüssel, von dieser zertifiziert werden. Ebenso benutzt die Zertifizierungsstelle ihren privaten Schlüssel für die Zertifizierung der öffentlichen Schlüssel der an dem Verfahren teilnehmenden Nutzer.

Teilnehmeridentifizierung und –registrierung

Prinzipiell ist die Erstellung eines Zertifikates für einen Teilnehmer oder eine Zertifizierungsstelle identisch. Als erstes muß jeder Teilnehmer seine Identität nachweisen[251]. Bei positiver Identifizierung wird ihm ein geeigneter und eindeutiger Name für die Unterschrift mittels digitaler Signatur zugewiesen[252]. Dabei ist es dem Teilnehmer freigestellt, ob er gegenüber Dritten mit seinem Namen oder einem Pseudonym auftreten möchte. Das Pseudonym läßt keinerlei Rückschlüsse auf die wahre Identität der Person zu, diese Verbindung kann jedoch von der Zer-

---

[248] Vgl. BSI (Signatur-Interoperabilitätsspezifikation, 1999), S. 30.

[249] Vgl. Kapitel 2.2.3.

[250] Die Gefährdungslage sowie Maßnahmen zur Absicherung sind wie beschrieben dem IT-Grundschutzhandbuch zu entnehmen, vgl. Kapitel 3.1.4.

[251] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 4;
Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 1.

[252] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 7.

tifizierungsstelle hergestellt werden. Nach der Identifizierung wird der Teilnehmer registriert[253].

Schlüsselerzeugung für die Teilnehmer

Sofern der Teilnehmer nicht bereits einen öffentlichen Schlüssel mitgebracht hat, muß im nächsten Schritt für den Teilnehmer ein Schlüsselpaar erzeugt werden[254], was in der Praxis den häufigeren Fall darstellen dürfte. Das erzeugte Paar darf mit keinem anderen Paar übereinstimmen[255] und muß zufällig sein, so daß es der Zertifizierungsstelle nicht möglich ist, dieses zu reproduzieren. Außerdem muß der generierte private Schlüssel seitens der Zertifizierungsstelle direkt nach der Übergabe vernichtet werden. Dadurch wird sichergestellt, daß nur das Original des privaten Schlüssels existiert[256].

Zertifikatserstellung

Nachdem der Teilnehmer identifiziert ist und der öffentliche Schlüssel feststeht, kann das Zertifikat erstellt werden. Um erstellte digitale Signaturen zweifelsfrei dem Teilnehmer zuordnen zu können, muß die Zuordnung des Schlüsselpaares ebenfalls zweifelsfrei erfolgen können[257]. Aus diesem Grund werden ein Identitätsmerkmal des Teilnehmers, sein öffentlicher Schlüssel, der Gültigkeitszeitraum und weitere Merkmale in einem Zertifikat zusammengefaßt. Dieses wird im Anschluß durch die Signatur der Zertifizierungsstelle, die durch den privaten Schlüssel der Zertifizierungsstelle erfolgen muß, unveränderbar, so daß die Inhalte authentisch

---

[253] Vgl. Harnier (Organisationsmöglichkeiten für Zertifizierungsstellen, 2000), S. 76.

[254] Vgl. Eckert (IT-Sicherheit, 2001), S. 273;
Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 8.
Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 2.

[255] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 4;
Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 8.

[256] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 7.

[257] Vgl. Thiel (Internationale Public-Key-Infrastrukturen aus Nutzersicht, 2000), S. 524.

miteinander verknüpft sind[258]. Das Zertifikat muß nach der Erstellung aufbewahrt und in den Verzeichnisdienst übernommen werden[259].

Personalisierung des Trägermediums

Im für den Teilnehmer letzten Schritt wird der private Schlüssel des Teilnehmers auf einem Trägermedium gespeichert[260]. Mit Hilfe dieses Mediums ist es dem Benutzer möglich, Dokumente digital zu signieren und verschlüsselte Dokumente zu entschlüsseln. Nach Möglichkeit ist auf dem Trägermedium die Benutzer-Authentifikation, die durch Eingabe eines Paßwortes oder einer Persönlichen Identifikationsnummer (PIN) erfolgen kann, zu aktivieren. Dies garantiert im Falle eines Verlustes des Trägermediums einen zusätzlichen Schutz vor Mißbrauch. Danach ist das Trägermedium dem Teilnehmer auszuhändigen[261].

Verzeichnisdienst

Im Verzeichnisdienst werden sämtliche öffentlich zugängliche Daten erfaßt und über Kommunikationseinrichtungen, beispielsweise das Internet, für jeden erreichbar gehalten[262]. Diese Daten umfassen zum einen die Schlüsselzertifikate aller Teilnehmer, zum anderen Sperrlisten[263], in denen alle ungültig gewordenen Zertifikate aufgeführt sind, um Teilnehmern eine Möglichkeit der Überprüfung der Gültigkeit eines Zertifikates zu schaffen[264]. Als Sperrinformation ist der Zeitpunkt der Sperrung des Zertifikates zu vermerken.

---

[258] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 7;
Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 4.

[259] Vgl. Stark/Biester/Fell/Volk u.a. (PKI Organisationshandbuch, 2001), S. 42.

[260] Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 4;
Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 7.

[261] Vgl. Harnier (Organisationsmöglichkeiten für Zertifizierungsstellen, 2000), S. 77.

[262] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 7.

[263] Vgl. Mack (Sperren von Zertifikaten, 2001), S. 465.

[264] Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 7.

Aus Datenschutzgründen dürfen die Zertifikate selbst beziehungsweise einzelne Informationen daraus, exemplarisch seien der Teilnehmername, das Pseudonym oder der öffentliche Schlüssel genannt, Dritten nur mit Erlaubnis des Teilnehmers zugänglich gemacht werden[265].

Zeitstempeldienst

Durch den Zeitstempeldienst werden beliebige Daten mit bestimmten Zeitpunkten verknüpft, so daß diese nachweisbar feststehen[266]. Dabei fügt der Zeitstempeldienst an ein beliebiges Dokument den aktuellen Zeitpunkt im Klartext an und signiert beides zusammen[267]. Wie beim Signieren ist hier ein Hashwert des zu zeitstempelnden Dokumentes ausreichend, um nicht unnötig viele Daten versenden zu müssen[268].

Die Zertifizierungsstelle benötigt den Zeitstempeldienst, um beispielsweise den Zeitpunkt der Sperrung eines Zertifikates nachweisbar dokumentieren zu können. Trotzdem ist nicht vorgeschrieben, daß eine Zertifizierungsstelle einen eigenen Zeitstempeldienst betreiben muß. Alternativ könnte die Zertifizierungsstelle diesen Dienst von einem Dritten, beispielsweise einer anderen Zertifizierungsstelle, ausführen lassen[269].

Sperrmanagement

Eine weitere Funktion einer Zertifizierungsstelle ist das Sperrmanagement. Jeder Teilnehmer muß jederzeit[270] die Möglichkeit haben, sein Zertifikat mittels eines

---

[265] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 5.

[266] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 6;
Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 8;
Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 7.

[267] Vgl. Harnier (Organisationsmöglichkeiten für Zertifizierungsstellen, 2000), S. 80.

[268] Vgl. Kapitel 2.2.4.

[269] Dies ergibt sich aus dem SigG §17 (3) und (4).

[270] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 52.

Anrufes sperren zu lassen[271], beispielsweise im Falle des Verlustes oder der Kompromittierung. Zu diesem Zweck muß eine Zertifizierungsstelle ein Call-Center betreiben, dessen Mitarbeiter den Benutzer mittels eines Paßwortes oder einer PIN identifiziert. Nach erfolgreicher Authentifizierung wird das Zertifikat gesperrt und in der nächsten Sperrliste veröffentlicht[272]. Hier wird deutlich, daß eine gewisse Zeitdauer zwischen dem Anruf, der Sperrung und der Veröffentlichung der Sperrliste vergehen muß, deren Ausmaß jedoch keinesfalls der Zertifizierungsstelle überlassen werden darf. Vielmehr müssen Regelungen für maximale Zeitspannen getroffen werden. Als realistisch kann beispielsweise eine Dauer von 10 Minuten zwischen der Authentifizierung des Teilnehmers und der Sperrung des Zertifikates[273] angenommen werden.

Sonstige Funktionalitäten

Zu den sonstigen Funktionalitäten einer Zertifizierungsstelle gehört die Datensicherung und –archivierung[274], der aufgrund der Brisanz der Daten eine entsprechende Bedeutung zukommt[275]. Eine detaillierte Beschreibung aller Prozesse und Sicherheitsmaßnahmen muß vorhanden sein und aufrechterhalten werden[276]. Ebenso ist ein Notfallmanagement zur Regelung nicht vorhersehbarer Ausnahmesituationen, beispielsweise durch Handlungsanweisungen, zu installieren und ein Reaktionsmechanismus für die Kompromittierung des Schlüssels der Zertifizierungsstelle beziehungsweise eines oder mehrerer Kryptoalgorithmen zu erarbeiten. Zusätzlich muß die im folgenden beschriebene Infrastruktur vor jeglichen Arten von Angriffen geschützt werden[277].

---

[271] Vgl. Schmeh (Kryptographie, 2001), S. 333.

[272] Vgl. Harnier (Organisationsmöglichkeiten für Zertifizierungsstellen, 2000), S. 79.

[273] Vgl. Bertsch/Pordesch (Problematik von Prozeßlaufzeiten, 1999), S. 515.

[274] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 67.

[275] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 6.

[276] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 54.

[277] Eine Klassifizierung der Angriffe folgt in Kapitel 4.4.

3.2.2 Infrastrukturkomponenten von Zertifizierungsstellen

Um die beschriebenen Funktionalitäten einer Zertifizierungsstelle nach den gültigen Gesetzen[278] gewährleisten zu können, muß die Infrastruktur bestimmte Voraussetzungen erfüllen[279].

Als erstes soll das Gebäude näher spezifiziert werden, in dem die Zertifizierungsstelle eingerichtet wird. Da alle Funktionalitäten mit Hilfe von Computern erbracht werden, folgt im nächsten Schritt die Erläuterung der benötigten Hardware. Danach wird die Software untersucht, wobei zum einen die der Zertifizierungsstelle und zum anderen die der Teilnehmer betrachtet wird. Des weiteren werden Anforderungen an die Bediensteten einer Zertifizierungsstelle beschrieben, bevor zum Schluß die Arbeitsanweisungen näher analysiert werden[280].

3.2.2.1 Gebäude

Weder das Signaturgesetz noch die Signaturverordnung machen Vorgaben dazu, wie ein Gebäude einer Zertifizierungsstelle auszusehen hat. Ganz allgemein wird von einem Gebäude gesprochen, das die notwendige Sicherheit für den Umgang mit Zertifikaten bietet.

Im Grundschutzhandbuch des BSI[281] finden sich ebenfalls keine Regelungen über den Bau eines solchen Gebäudes. Vielmehr werden sämtliche Bedrohungen[282] für Gebäude aufgezählt und Maßnahmen aufgeführt, die Schutz vor solchen Bedrohungen bieten beziehungsweise die Wahrscheinlichkeit des Schadeneintritts oder

---

[278] Vgl. Kapitel 3.1. Dies sind die Europäische Signaturverordnung, das Signaturgesetz, die Signaturverordnung und das IT-Grundschutzhandbuch des BSI.

[279] Vgl. Robben (Digitale Signatur, 2000), Internet-Quelle.

[280] Die Spezifizierung des beschriebenen Gebäudes richtet sich nach Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), einer Anwendung des IT-Grundschutzhandbuches auf Zertifizierungsstellen.

[281] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Internet-Quelle.

[282] Im Gefährdungskatalog höhere Gewalt, vgl. Kapitel 3.1.4, sind dies zum Beispiel Blitz, Feuer und Wasser. Für sämtliche Bedrohungen vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 4.1.

das Schadenausmaß verringern. Als erster Vorschlag wird das in Abbildung 3-4 dargestellte vom BSI skizzierte Gebäude als Infrastruktur für Zertifizierungsstellen verwendet[283].

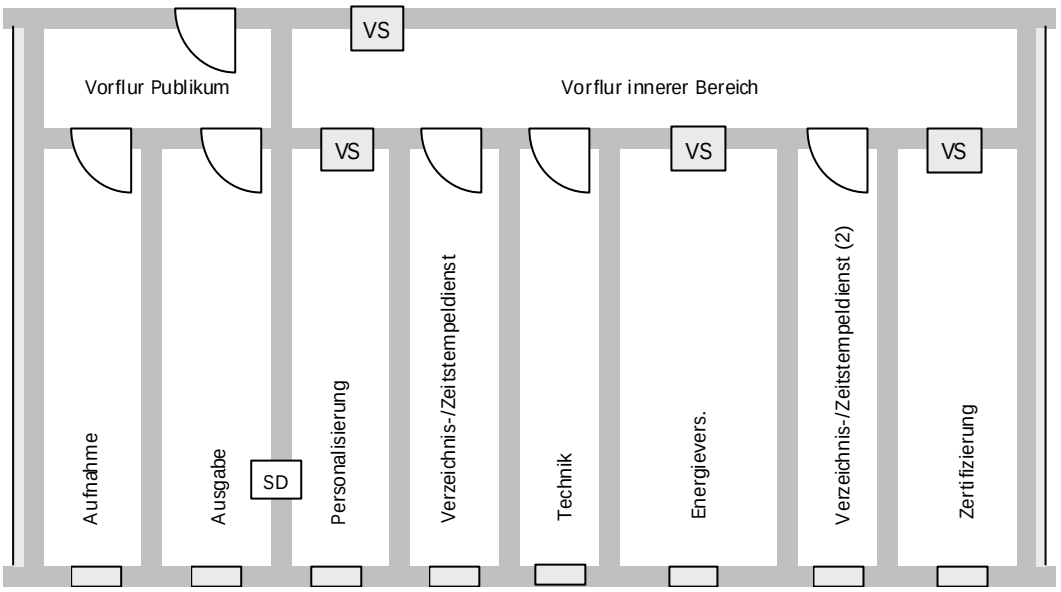

Abbildung 3-4 – Raumaufteilung einer möglichen signaturgesetzkonformen Zertifizierungsstelle

Quelle: Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 2.

Hinter dem Publikumsflur befinden sich die Zimmer für die Annahme der Anträge und Ausgabe der personalisierten Trägermedien. Dabei werden die Trägermedien mittels einer Durchreiche aus der Personalisierung, die sich in dem nicht für Besucher zugänglichen Teil des Gebäudes befindet, überbracht. Sie ist zusätzlich, ebenso wie der Zertifizierungsraum am anderen Ende des Flurs, durch eine Personenschleuse mit dem Flur verbunden. Dazwischen liegen die beiden Räume des Verzeichnis- und Zeitstempeldienstes, die jeweils doppelt vorhanden sind. Zwischen beiden befindet sich der Technikraum und der Raum für die Energieversorgung, der das Notstromaggregat enthält.

Für Mauern der Räume sind Mindestvorgaben bezüglich Dicke und Druckfestigkeit einzuhalten[284]. Besonders ist darauf zu achten, daß alle Wände vom Fußboden

[283] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 2ff.

bis zur Decke reichen, um nicht durch abgehängte Decken Lücken zu schaffen. Innerhalb aller Wände, zumindest von jedem genannten Raum zum Raum Technik und Energieversorgung, sollten Leerrohre zur Verkabelung der Rechner verlegt werden. Innerhalb der Räume kann auf andere Kabelkanäle ausgewichen werden[285].

Türen[286], Vereinzelungsschleusen (VS)[287] und Fenstern[288] kommt besondere Bedeutung zu, da es sich im Gegensatz zu Wänden um primäre Angriffsziele handelt[289]. Neben der Einhaltung von Sicherheitsklassen für Rahmen, Türen beziehungsweise Verglasung und Schlössern sind Alarmanlagen und Durchbruchüberwachungen zu empfehlen. Bei den Fenstern kommt zum ersten Mal der Konflikt zwischen der zu

---

[284] Auf die detaillierten Angaben soll im Text verzichtet werden. In diesem Fall muß das Mauerwerk nach DIN 1093 Teil 1 mit einer Nenndicke von mindestens 240 mm und Steinen der Druckfestigkeitsklasse 12 und Mörtel der Gruppe II gefertigt werden. Alternativ ist auch Stahlbeton nach DIN 1045 der Festigkeitsklasse B 15 oder höher mit einer Nenndicke von mindestens 140 mm zu verwenden.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 2.

[285] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 3.

[286] Sicherheitsklasse ET 3 nach DIN V 18103, zusätzlich Erfüllung der Anforderungen einer Brandschutztür der Klasse T 90 nach DIN 4102 Teil 5.
Schlösser der Klasse 4 nach DIN 18251 mit Zylindern der Klasse 3 nach DIN V 18254/07.91 Abschnitt 6.4 mit Kugelzuhalterungen und Schutzbeschlägen der Klasse ES 3 nach DIN 18257 mit Kernziehschutz.
Eingebaute Magnet- und Riegelkontakte sollten auf Öffnen und Verschluß überwacht werden und mit dem Verriegelungssystem HZ-Lock der Firma Hellmüller + Zingg oder gleichwertig ausgestattet sein.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 3.

[287] Diese sollten Anforderungen der Türen der Widerstandsklasse ET 3 nach DIN V 18103 samt Prüfzeugnis entsprechen, Schleusen mit Durchbruchüberwachung.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 3.

[288] Alle Fenster sollten Konstruktionen der Klasse EF 3 nach DIN V 18054 mit Verglasung der Klasse B 3 gemäß DIN 52290 Teil 3 und Durchbruchüberwachung sein.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 3.

[289] Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 9.

erreichenden Sicherheit und Anforderungen beziehungsweise Wünschen der Benutzer zum Vorschein, da Fenster gegenüber einer Wand sicherlich weniger Schutz bieten. Allerdings müßten dann alle dort arbeitenden Personen permanent ohne Tageslicht auskommen.

Als letztes soll die Sicherheitsdurchreiche (SD) untersucht werden, die ebenfalls durch eine Durchbruchüberwachung geschützt werden sollte. Da an dieser Stelle der dem Publikum zugängliche Teil der Zertifizierungsstelle von dem nicht zugänglichen getrennt ist, muß die Durchreiche das Einbringen von Brandbeschleunigern und Explosivstoffen verhindern. Dies könnte durch eine Sicherheitsschiebemulde erreicht werden. Um Mißbrauch personalisierter Medien auszuschließen, sollte die Ausgabe von der Personalisierung einsehbar sein, realisierbar durch halbdurchlässige Verglasung[290] oder Videotechnik[291].

3.2.2.2 Gebäudesicherung

Die Gebäudesicherung umfaßt neben dem Gebäudeschutz die Zugangskontrolle, den Brandschutz[292], die Einbruchmeldeanlage[293], den Wasserschutz[294] und die Kühlung[295].

---

[290] Verglasung EF3/B3. Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 4.

[291] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 4.

[292] Die Brandschutzmeldeanlage sollte der VdS-Anforderung 2095 und den Anschaltbedingungen der örtlichen Feuerwehr genügen. Das VdS-Merkblatt zum Brandschutz in Räumen für elektronische Datenverarbeitungsanlagen (Nr. 2007) sollte ebenfalls berücksichtigt werden.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 12.

[293] Die Einbruchmeldeanlage sollte den Anforderungen des BSI an Alarmanlagen für Einbruch und Überfall (BSI 7510) der jeweils gültigen Fassung genügen.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 14.

[294] Dies schließt 10 cm Bodenfreiheit, Wassermeldesysteme und Handpumpen zur Entwässerung ein. Räume, die tiefer als 1 m über Kanalisationsniveau liegen, benötigen Rückstauventile in den Abwasserleitungen und automatische Entwässerungspumpen. Höher liegende Räume sollten über eine selbstständige Entwässerung verfügen.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 15.

Unter Gebäudeschutz ist zu verstehen, daß insbesondere außerhalb der Öffnungszeiten der Zertifizierungsstelle ein Wachdienst außerhalb und innerhalb des Gebäudes patrouilliert, um verdächtige Personen zu erkennen und Angriffe zu verhindern. Diese Maßnahmen ergänzen die elektronische Überwachung des Gebäudes mit Video- und Wärmebildkameras[296].

Die Zugangskontrolle des Gebäudes spielt die wichtigste Rolle. An sämtlichen Türen zum Inneren der Zertifizierungsstelle müssen eigenständige Zugangskontrolleinheiten angebracht werden, die entweder mit biometrischen Lesern oder Chipkartenlesern in Verbindung mit einer PIN ausgestattet sind. An Türen mit Vereinzelungsschleusen sollten diese Leser zusätzlich für die Ausgangskontrolle eingesetzt werden. Die Zentrale und der Administrationsplatz sollte sich im Raum Technik befinden. Als wichtigste Funktion ist der interne Speicher der Auswertungseinheit für Berechtigungs- und Protokolldaten zu nennen. Die Zutrittsrechte werden durch den Administrator vergeben[297].

Besucher dürfen sich innerhalb der Zertifizierungsstelle nur bewegen, wenn ihre Besucherberechtigung schriftlich erteilt und protokolliert wurde und sie permanent von einem Mitarbeiter der Zertifizierungsstelle begleitet werden, der über die

---

[295] Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 9;
Um eine Abführung der Abwärme der IT-Systeme zu gewährleisten, sollte eine Wärmelastberechnung durchgeführt werden. Sollten einzelne Räume eine Kühlung benötigen, so sind für redundante Komponenten wie den Verzeichnis- oder Zeitstempeldienst auf jeden Fall getrennte Geräte vorzusehen. Überschreitungen der Betriebstemperatur müssen angezeigt werden.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 15.

[296] Vgl. Schuhmacher (Wirtschafts- und Wettbewerbsspionage, 2001), Internet-Quelle.

[297] Weitere Mindestfunktionen sind Türoffenzeitüberwachung, Schnittstelle zum Bedienplatz der Besuchererfassung und für die Leser an den IT-Systemen der Zertifizierungsstelle, Möglichkeit der Plausibilitätskontrolle zwischen Zutrittsschutz und Zugangsschutz, Energieversorgung der Leser von der Zentrale und eine Notstromversorgung für mindestens 72 Stunden oder eine Aufschaltung auf die NEA mit Schaltüberbrückung für 5 Minuten.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 9.

benötigten Zutrittsrechte verfügt. Die Besucher sind mit einem Ausweis auszustatten. Die Mitarbeiter der Besuchererfassung[298] dürfen in keinem Fall mit der Administration der Zugangsberechtigungen betraut sein[299]. Um den kontrollierten Einlaß in den Publikumsbereich sicherzustellen, müssen am Zugang zum Vorflur Publikum sowie in den Räumen Annahme und Ausgabe Videosprechstellen angebracht und deren Zentrale ebenfalls im Raum Technik installiert werden[300].

Der Brandschutz der Zertifizierungsstelle ist aufgeteilt in die allgemeine Brandüberwachung, die Objektbrandüberwachung[301] und die Löschung. Die für die Sicherheit und Funktion der Zertifizierungsstelle notwendigen und daran angrenzenden Räume der Zertifizierungsstelle sind mit einer Brandmeldeanlage (BMA)[302] zu überwachen, die direkt an die Einsatzstelle der örtlichen Feuerwehr aufgeschaltet ist und deren Zentrale sich im Raum Technik befindet. In allen anderen Räu-

---

[298] Der Raum der Besuchererfassung muß in den Brandschutz mit einbezogen werden und gegen unberechtigten Zutritt gesichert sein. Die Besucherausweise in diesem Raum sollten in einem VS-Schlüsselbehälter nach BSI 7570 aufbewahrt werden. Besucher sollten biometrisch erfaßt werden. Die Besucherberechtigungen sollten auf einen Tag beschränkt und der Zutritt eines Raumes nur innerhalb eines Zeitfensters von 20 Sekunden nach dem Zutritt des berechtigten, ständig begleitenden Mitarbeiters möglich sein. Neben der technischen und organisatorischen Besucherregelung sollte vorgesehen sein, daß jeder Zutrittsberechtigte nur maximal einen Besucher begleitet.

Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 10.

[299] In diesem Fall wird deutlich, daß erhöhte Sicherheit mit einem erhöhten Personaleinsatz und damit höheren Kosten einhergeht.

[300] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 10.

[301] Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 10.

[302] Es ist sicherzustellen, daß die BMA der VdS-Anforderung 2095 (Richtlinien für automatische Brandmeldeanlagen – Planung und Einbau) und den Anschaltebedingungen der örtlichen Feuerwehr genügen. Des weiteren ist sie direkt auf die Feuerwehr aufzuschalten und im Raum Technik unterzubringen.

Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 12.

men des inneren Bereiches ist eine Objektbrandüberwachung[303] vorgesehen, deren Meldestufen zu einer gestaffelten Alarmreaktion genutzt werden sollten. Die Kabel sollten 90 Minuten Funktionserhalt bieten. Bei der Löschung ist Objektlöschung einer Löschung durch die Feuerwehr oder einer zentralen Löschanlage aufgrund der extrem hohen Verfügbarkeitserwartungen vorzuziehen. Alle Geräte mit Objektbrandüberwachung sollten deshalb mit einer Gerätelöscheinrichtung versehen, die Bereiche der Energieversorgung mit einer Raum-Gas-Löschanlage[304] ausgestattet sein[305].

Entsprechend den Anforderungen des BSI an Alarmanlagen für Einbruch und Überfall[306] in der jeweils gültigen Fassung muß die Einbruchmeldeanlage geplant und eingesetzt werden. Sämtliche Räume sind mit einer Volumenüberwachung auszustatten, die durch mindestens 2 Bewegungsmelder realisiert wird und bei der sich jeder im Erfassungsbereich mindestens eines anderen befindet. Für Fenster, Vereinzelungsschleusen und die Sicherheitsdurchreiche muß eine Durchbruchüberwachung existieren. Alarme sollten als Störmeldungen an geeigneter Stelle[307] angezeigt werden. Die Zentrale ist ebenso im Raum Technik unterzubringen. Alle überwachten Räume sollten als Scharfschaltebereiche ausgeführt werden, so daß die Blockschloßfunktion eine Türöffnung bei scharfgeschaltetem Raum unterbindet[308].

Um genügenden Schutz gegen eindringendes Wasser zu gewährleisten, sollte sämtlichen IT-Geräten mindestens 10 cm Bodenfreiheit gewährt werden. Darüber hin-

---

[303] Die Meldestufen der Objektmelder sollten zu einer objektbezogenen Alarmreaktion genutzt werden, die durch einen Voralarm, das Spannungsfrei-Schalten des betroffenen Gerätes, die Objektlöschung und den Hauptalarm an die Feuerwehr gestaffelt ist.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 12.

[304] Die Löschung sollte in 2-Linienabhängigkeit durch die BMA oder Handauslösung angesteuert werden. Die Auslösung muß an geeigneter Stelle angezeigt werden.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 13.

[305] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 12.

[306] Spezifiziert in BSI 7510.

[307] Eine Aufschaltung an die Polizei ist möglich.

[308] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 14.

aus sind automatische Entwässerungspumpen und Handpumpen vorzusehen[309]. Schutz vor Überhitzung der IT-Systeme ist durch Wärmeabfuhrsysteme zu gewährleisten, deren Leistung die in der Wärmelastberechnung ermittelten Maximalwerte übersteigt. Für beide Verzeichnis- und Zeitstempeldiensträume sind getrennte Geräte vorzusehen. Eindringendes Wasser oder Überschreitungen der zulässigen Betriebstemperatur sind an geeigneter Stelle anzuzeigen[310].

3.2.2.3 Energieversorgung

Schon am Gebäude der Zertifizierungsstelle werden die hohen Verfügbarkeitsanforderungen sichtbar, die aufgrund der elektronischen Dienstleistungen ebenfalls für die Energieversorgung[311] gelten müssen. Die Grundlage der Stromverteilung bildet die Niederspannungshauptversorgung (NHV), für die aufgrund dieser zentralen Bedeutung besondere Vorkehrungen hinsichtlich des Zutrittsschutzes und des Brandschutzes getroffen werden müssen[312]. Die gesamte Zertifizierungsstelle sollte als Blitzschutzzone 2 ausgelegt werden[313]. Daraus resultieren die Erarbeitung eines Überspannungsschutzkonzeptes und der Einsatz von Überspannungsschutzeinrichtungen für sämtliche Leitungen[314] ab der NHV[315].

---

[309] Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 10.

[310] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 15.

[311] Die Energieversorgung sollte 5-drähtig als TN-S-Netz konzipiert werden.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 5.

[312] Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 9.

[313] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 8.

[314] Für diese Kabel gelten die Anforderungen der DIN 4102 Teil 12 Funktionserhaltklasse E90. Des weiteren sollten sie über die gesamte Länge ungeschnitten und außerhalb der Zertifizierungsstelle durch Verlegung in zutrittgeschützten Bereichen und Stahlpanzerrohren gegen Beschädigungen geschützt werden.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 5.

Wie in der Gebäudeskizze eingezeichnet ist der Zutritt zu diesem Raum nur über eine Vereinzelungsschleuse möglich. Auf das Fenster könnte verzichtet werden, jedoch wäre in diesem Fall von außen ersichtlich, um welchen Raum es sich handelt. Aus diesem Grund darf keine Unterscheidung vorgenommen werden. Es bestünde die Möglichkeit, die Energieversorgung in einem getrennten Gebäude unterzubringen, jedoch müßten in diesem Fall die Stromleitungen zwischen den Gebäuden verlaufen, so daß neue Angriffspunkte entstünden[316].

Des weiteren muß eine Netz-Ersatzanlage (NEA) existieren, die mit Treibstoff betrieben wird und für mindestens 6 Stunden den benötigten Strom liefern kann. Die zu erwartende Endauslastung muß mindestens über dem Faktor 1,5 liegen und die Treibstoffzufuhr über diesen Zeitrahmen hinweg organisatorisch sichergestellt werden[317]. Bei Ausfall der Niederspannungshauptversorgung muß die Umschaltung auf die Netz-Ersatzanlage automatisch erfolgen. Die Umschalteinrichtung muß außerdem in einem separaten Brandabschnitt untergebracht werden[318], der mittels einer Abmauerung oder eines geeigneten Behälters hergestellt werden kann. Alle Räume und eventuell auch Schränke müssen in die allgemeine Brandüberwachung einbezogen und auf Verschluß überwacht werden[319].

Sämtliche Versorgungsleitungen von der Niederspannungshauptverteilung und der Netz-Ersatzanlage zur Technik sollten doppelt und durch unterschiedliche Brandbereiche verlegt werden, sofern dies möglich ist[320]. Eine permanente Überwachung beider Leitungen ist vom Raum Technik aus zu ermöglichen. Vom dort aus er-

---

[315] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 5;
Vgl. Becker/Dusemund/Gollan/Engel/Meinel (Infrastructure, Specifications and Standards, 2000), S. 10.

[316] Schutzmaßnahmen in diesem Fall sind weiter oben in den Fußnoten erläutert.

[317] Qualität und Ausstattung werden ausreichend durch T30 beschrieben.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 6.

[318] Die Tür des Raumes oder Schrankes der Umschalteeinrichtung sollte auf Verschluß überwacht werden damit der Brandschutz (F90) sichergestellt werden kann.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 6.

[319] Vgl. ebenda.

[320] Vgl. ebenda.

folgt, wie oben bereits bei der Verkabelung erwähnt, die Verteilung in die anderen Räume. Die Verteiler in den einzelnen Räumen müssen überwacht und mit eigenen Löscheinrichtungen ausgestattet sein. Alle Versorgungsleitungen müssen unabhängig voneinander gesichert werden. Die für die Zertifizierungsstelle erforderlichen IT-Systeme sollten mittels Festanschluß mit Strom versorgt werden, so daß kein versehentliches Lösen von Verbindungen am Gerät möglich ist[321].

Für die in den Räumen des Verzeichnis- und Zeitstempeldienstes installierten IT-Systeme sollte darüber hinaus eine lokale Unterstromversorgung (USV) eingerichtet werden, die per ausschließlich anzeigender Fernwartungssoftware kontrolliert wird. Die benötigte Leistung sollte wiederum mindestens die 1,5-fache maximale Endauslastung abdecken und für das 10-fache der maximal zu erwartenden Umschaltdauer ausgelegt sein. Ähnlich den Verteilungssystemen sollten Objektbrandüberwachung und Objektüberwachung für alle USV-Geräte vorhanden sein[322].

3.2.2.4 Hardware und Software

Da sämtliche Dienstleistungen einer Zertifizierungsstelle von IT-Systemen erbracht werden, muß die Hard- und Software höchsten Ansprüchen an die Verfügbarkeit genügen. Um Hardware-Ausfällen vorzubeugen, müssen demnach möglichst viele Komponenten redundant ausgelegt sein[323]. Des weiteren müssen sämtliche Komponenten schnell austauschbar sein, um im Fehlerfall eine rasche Wiederherstellung der Funktionsfähigkeit erreichen zu können. Der benötigte Strom wird mittels des Energiemanagements garantiert[324].

---

[321] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 7.

[322] Es ist sicherzustellen, daß der erforderliche Crest-Faktor eingehalten wird.
Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 7.

[323] Je mehr Komponenten redundant sind, desto höher ist die Wahrscheinlichkeit, daß ein IT-System trotz des Defektes einer Komponente stabil weiterläuft. Eine Komponente redundant zu gestalten, schlägt sich jedoch mindestens in den doppelten Kosten nieder, da die Komponente doppelt benötigt wird und eventuell noch eine Steuerung vorhanden sein muß.
Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 67.

[324] Vgl. Kapitel 3.2.2.3.

Neben der Verfügbarkeit müssen die Daten der IT-Systeme sicher gegen jegliche Art von Angriffen sein[325]. Während der physische Zugriff auf die Hardware durch die Gebäudesicherheit und Zugriffskontrollen garantiert wird, bietet die Abstrahlung der Rechner sowie der Verkabelung Abhörmöglichkeiten[326]. Durch entsprechende Verkabelung[327] und Rechnergehäuse sowie bauliche und organisatorische Maßnahmen kann dies verhindert werden[328].

Einfacher als im Falle der Hardware stellt sich das Design der Software dar, weil die geforderten Sicherheitsbedürfnisse nur bei der Entwicklung zu berücksichtigen sind. Die Zertifizierungsstelle steht vor der Wahl, eine Software zu kaufen, die mindestens sämtliche gesetzlichen Anforderungen erfüllt, eine Individualentwicklung in Auftrag zu geben oder die Software selbst zu entwickeln. Die letzte Möglichkeit ist wenig wahrscheinlich, da die dafür benötigten Entwickler nicht im erforderlichen Ausmaß zur Verfügung stehen dürften.

Als Anforderung der Software ist als wichtigste die Zugriffssteuerung der Benutzer zu nennen[329]. Die Authentifizierung der Benutzer muß mittels eines geeigneten Verfahrens, exemplarisch seien biometrische oder PIN-basierte Verfahren genannt, erfolgen. Zusätzlich muß es möglich sein, sicherheitskritische Funktionen nur zuzulassen, wenn sie von zwei Benutzern mit entsprechender Legitimation autorisiert werden[330]. Jede Aktion eines Benutzers muß protokolliert werden, ohne daß diese Log-Einträge vom Benutzer löschbar sind[331].

Schon aufgrund der Erstinvestition muß eine Zertifizierungsstelle den Verkauf vieler Zertifikate zum Ziel haben. Die Software und ihre Bedienung muß aus die-

---

[325] Eine Klassifizierung der Angriffe findet in Kapitel 4.4 statt.

[326] Vgl. Schmid (ECHOLON, 2001), S. 26ff.

[327] Entsprechend wäre beispielsweise der Einsatz von Glasfaser-Lichtwellenleitern.

[328] Weitere Angaben zur Abstrahlsicherheit bietet BSI (IT-Grundschutzhandbuch, 2001), M4.89. Erläuterungen zur Auswahl der Kabel finden sich in BSI (IT-Grundschutzhandbuch, 2001), M5.3.

[329] Dies ergibt sich aus BSI (IT-Grundschutzhandbuch, 2001), M4.1, M4.14-M4.17, M4.27 etc.

[330] Dies schafft eine zusätzliche Kontrollinstanz.

[331] Auf diese Weise läßt sich jede Manipulation zumindest nachträglich nachweisen.

sem Grund auf eine große Anzahl, etwa eine Millionen Zertifikate, ausgelegt sein. Weil sich die Anzahl der Zertifikate im Laufe der Zeit erhöht, wächst der Bedarf an Sperrungen. Somit müssen die Sperrkomponenten skalierbar ausgelegt sein. In geringerem Maße trifft dies ebenfalls auf die Kollektoren zur Eingabe von Zertifikaten zu[332].

Darüber hinaus muß die Software und die auf den Rechnern der Teilnehmer installierte Clientsoftware verschiedene Algorithmen unterstützen, die leicht austauschbar sein müssen[333], da die Algorithmen nur für einen begrenzten Zeitraum als sicher angesehen werden[334]. Die gesetzliche Vorgabe sieht nur die Nutzung eines Algorithmus vor, jedoch bietet die Nutzung multipler Algorithmen im Fall der Kompromittierung Vorteile, weil die Infrastruktur mittels der zusätzlichen Algorithmen aufrechterhalten werden kann[335] und kein Vertrauensverlust der Teilnehmer eintritt[336]. Der für die Zertifizierungsstelle wichtigste Vorteil ist die Kostenersparnis beim Austausch der betroffenen Teilnehmerzertifikate und der Clientsoftware, weil eine funktionsfähige Infrastruktur auf Basis des Ausweichalgorithmus bestehen bleibt, die genutzt werden kann.

3.2.2.5 Personal

Weil nicht alle Prozesse der Zertifizierungsstelle vollständig automatisiert ablaufen, sind die Mitarbeiter für den reibungslosen Ablauf der Prozesse entscheidend. Neben der Qualifikation und Zuverlässigkeit der Mitarbeiter ist die Anzahl der Mitarbeiter, beispielsweise im Bereich der Zertifikatssperrung, von enormer Be-

---

[332] Um Engpässe zu vermeiden, müssen Endgeräte nachträglich hinzugefügt werden können.

[333] Vgl. Hartmann/Maseberg (Fail-Safe-Konzepte für FlexiPKI, 2002), S. 4.

[334] Vgl. Bundesanzeiger (Geeignete Kryptoalgorithmen, 2000);
Vgl. SigV §17 (2).

[335] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 115.

[336] Der Vertrauensverlust tritt ein, weil die Infrastruktur nicht mehr sicher ist und die Sicherheit erst wieder hergestellt werden muß.

deutung[337]. Für die Zertifizierungsstelle aufgrund der anfallenden Kosten, für die Nutzer in Form von Wartezeiten.

Die Zertifizierungsstelle hat bezüglich Zertifikatssperrung viele Möglichkeiten. Während das Signaturgesetz[338] beziehungsweise die Spezifizierung in der Signaturverordnung[339] eine Möglichkeit der Sperrung über eine Rufnummer 24 Stunden an jedem Tag vorschreibt, wäre eine niedrigere Sperrzeit für nicht signaturgesetzkonforme Zertifizierungsstellen möglich. Diese könnte beispielsweise nur während der normalen Bürozeiten möglich sein. In diesem Fall wäre ein Mitarbeiter samt Vertretung ausreichend. Um jeden Tag 24 Stunden eine Zertifikatssperrung zu ermöglichen, sind mindestens fünf Mitarbeiter notwendig, wenn die Wochenarbeitszeit unter 42 Stunden liegen soll. Dies schließt Feiertage, Urlaub und Krankheit der Mitarbeiter noch nicht mit ein. In beiden Fällen könnte eine zeitgleiche Sperrung von zwei oder mehr Zertifikaten nicht stattfinden, so daß ein Teilnehmer warten müßte. Für die Zertifizierungsstelle bedeutet dies ein zusätzliches Risiko, da der Teilnehmer im Schadensfall die Zertifizierungsstelle haftbar machen könnte[340].

Die Sicherheit der von der Zertifizierungsstelle ausgestellten Zertifikate wird jedoch hauptsächlich von der Policy bestimmt, die detaillierte Arbeitsanweisungen aller Prozesse enthält und Richtlinien für den Umgang mit Zertifikaten vorgibt.

---

[337] Eine genauere Darstellung der benötigten Mitarbeiter und ihrer Rollen findet sich in Kapitel 5.2.1.5.

[338] Vgl. SigG §8.

[339] Vgl. SigV §7.

[340] Eine detailliertere Darstellung dieses Sachverhalts findet sich in Kapitel 3.2.1.

4 Rahmenbedingungen für Zertifizierungsstellen

Beim Aufbau einer eigenen Zertifizierungsstelle ist zunächst zu klären, ob Signaturgesetzkonformität erreicht werden soll oder nicht. Im ersten Fall sind dadurch nahezu alle Anforderungen an Zertifizierungsstellen festgelegt, im zweiten Fall stehen sämtliche Möglichkeiten offen.

Gerade aufgrund der kostenintensiven Infrastruktur einer signaturgesetzkonformen Zertifizierungsstelle[341] stellt sich jedoch die Frage, wieviel kostengünstiger der zweite Fall zu realisieren ist. Da die Vorteile qualifizierter Zertifikate freiwillig akkreditierter Anbieter in Form des Anscheinsbeweises[342] gegenüber allen anderen Zertifikaten groß sind, muß der Preisvorteil ebenfalls spürbar sein, um den Zusatznutzen auszugleichen. Als wichtigste zu betrachtende Rahmenbedingungen sind das Vertrauensmodell und das Klassifizierungskriterium der Zertifikate zu nennen, die in den ersten beiden Abschnitten dieses Kapitels behandelt werden. Im dritten Abschnitt erfolgt eine Betrachtung der notwendigen Prozesse einer Zertifizierungsstelle, im vierten Abschnitt eine Klassifikation der Angriffe auf eine Public-Key-Infrastruktur. Die Einsatzmöglichkeiten von Zertifikaten werden im letzten Abschnitt untersucht.

4.1 Vertrauensverfahren

Um die in den technischen Grundlagen vorgestellte asymmetrische Verschlüsselung zum sicheren Übertragen und Signieren von Daten nutzen zu können, muß

[341] Vgl. Fox (Preis der Pioniertat, 2001), S. 62.

[342] Vgl. Harnier (Organisationsmöglichkeiten für Zertifizierungsstellen, 2000), S. 54.

Vertrauen zu einem Zertifikat bestehen, das die Identität einer Person an einen öffentlichen Schlüssel bindet.

Ob die ebenfalls vorgestellten Zertifizierungsstellen benötigt werden, soll in den folgenden Abschnitten ermittelt werden. Begonnen wird mit der Darstellung von Vertrauensverfahren für Personen, die ohne Zertifizierungsstellen auskommen, bevor diese im nächsten Abschnitt in die Überlegungen einbezogen werden. Die Sicherheit, mit der einem fremden Zertifikat vertraut werden kann, dient als Kriterium der Beurteilung der Modelle.

4.1.1 Vertrauensverfahren für Personen

Am sichersten ist es, nur Zertifikaten zu vertrauen, die persönlich per Diskette oder anderen Datenträgern übergeben und eingespielt werden, da keine weiteren Personen eingebunden sind, die Manipulationen vornehmen könnten. Dieses Verfahren des direkten Vertrauens ist im Internet nicht praktikabel, weil in diesem Fall die Ortsunabhängigkeit aufgehoben würde. Das Vertrauensverhältnis dieses Verfahrens wird durch Abbildung 4-1 verdeutlicht.

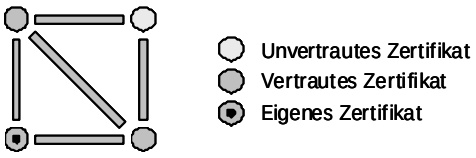

Abbildung 4-1 – Direktes Vertrauen

Um diese Probleme zu umgehen, wurde von dem Programm Pretty Good Privacy (PGP)[343] das Netz des Vertrauens (Web of Trust) eingeführt[344]. Hier vertraut ein Teilnehmer nicht nur den direkt erhaltenen Zertifikaten, sondern zusätzlich allen

[343] Urspünglich von Phil Zimmermann geschriebene Software zum Verschlüsseln von Mails.
Vgl. o.V. (PGP, 2001), Internet-Quelle;
Vgl. Fuhrberg, Kai (Internet-Sicherheit, 1998), S. 103.

[344] Vgl. o.V. (How PGP works, 2001), Kapitel Trust models;
Vgl. Schmeh (Kryptographie, 2001), S. 283ff.

Zertifikaten, denen dessen Inhaber vertrauen[345] und dieses Vertrauen kann beliebig fortgesetzt werden[346]. Nachteile bei dieser Vorgehensweise sind die Tatsachen, daß zum einen lange Ketten[347] benötigt werden, um das gewünschte Zertifikat zu erhalten[348] und zum anderen, daß ein Angreifer es nur erreichen muß in die Kette zu gelangen, um nicht vertrauenswürdige Zertifikate einzuschleusen[349]. Diese Vertrauenssituation ist in Abbildung 4-2 abgebildet.

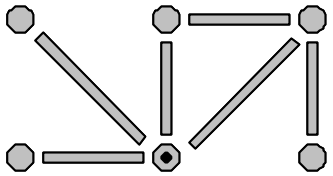

Abbildung 4-2 – Netz des Vertrauens (Web of Trust)

Eine Möglichkeit, potentiellen Angreifern dies zu erschweren, ist die Einführung einer Abstufung des Netzes, so daß unbekannten Zertifikaten nicht automatisch Vertrauen geschenkt wird. Vielmehr würde eine Grenze definiert, ab wann Zertifikate Vertrauen im Netz erhielten. Eine Abstufung auf beispielsweise zwei Wege hätte zur Folge, daß nur Zertifikaten vertraut wird, die auf zwei unterschiedlichen Zertifikatsketten erreichbar sind. Es müssen demnach für jedes Zertifikat innerhalb der Kette jeweils zwei Teilnehmer gefunden werden, die diesem vertrauen. Sollte dies das gewünschte Sicherheitsniveau nicht herstellen, so kann die Zahl der

---

[345] Das von PGP tatsächlich realisierte Modell ist wesentlich komplexer. Die prinzipielle Funktionsweise ist an dieser Stelle jedoch ausreichend. Einen Einstieg in die genaue Funktionsweise von PGP bietet:
Vgl. o.V. (How PGP works, 2001), Kapitel Levels of trust in PGP.

[346] Vgl. Merz (Electronic Commerce, 1999), S. 138;
Vgl. Perlman (An Overview of PKI Trust Models, 1999), S. 40.

[347] PGP nennt die Zahl von sechs Intermediären, die benötigt werden, um zwei beliebige Personen dieser Welt über Zertifikate zu verbinden. Selbst bei dieser optimistischen Annahme bleiben demnach sechs Personen, denen vertraut werden muß.
Vgl. o.V. (How PGP works, 2001), Kapitel Web of Trust.

[348] Vgl. Fox (Cross-Zertifikat, 2001), S. 105.

[349] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 141.

benötigten Teilnehmer erhöht werden, mit der Folge einer sinkenden Zahl an vertrauten Zertifikaten. Eine graphische Abbildung dieser Vertrauensverhältnisse findet sich in Abbildung 4-3.

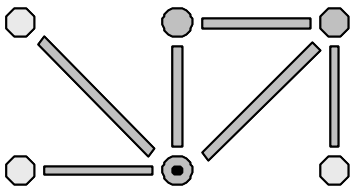

Abbildung 4-3 – Netz des Vertrauens (Abgestuft auf 2 Wege)

Um die Länge der Zertifikatsketten zu verkürzen, müssen andere Strukturen als Netze benutzt werden[350]. Eine Möglichkeit dies zu erreichen sind Bäume, sofern diese ausbalanciert sind. Dabei entstehen Hierarchien, bei denen einzelnen Zertifikaten größere Bedeutung zukommt als anderen. Dieses zusätzliche Vertrauen muß unter anderem durch höhere Sicherheit gerechtfertigt werden. Abbildung 4-4 zeigt das Vertrauensverhältnis einer Hierarchie.

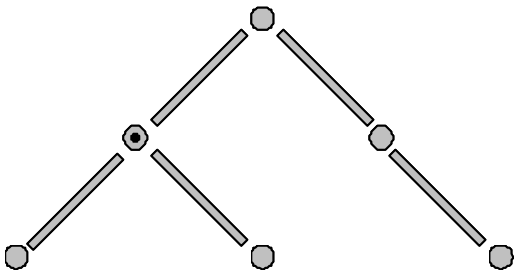

Abbildung 4-4 – Vertrauenshierarchie

Problematisch ist bei diesem Ansatz, welche Teilnehmer mit ihren Zertifikaten über anderen stehen sollen oder ob das tragbare Risiko nicht überschritten wird. Daraus wird ersichtlich, weshalb Zertifizierungsstellen diese Rolle übernehmen können.

[350] Vgl. Hammer (Cross-Zertifikate verbinden, 2001), S. 66.

4.1.2 Vertrauensverfahren für Zertifizierungsstellen

Neben der höheren Sicherheit, die Zertifizierungsstellen gegenüber Individuen bieten, gibt es weitere Gründe, die für deren Einsatz sprechen. Als wichtigster ist die Behandlung von abgelaufenen Zertifikaten, insbesondere von revozierten Zertifikaten, die beispielsweise aufgrund eines Verlustes der Chipkarte unsicher geworden sind, zu nennen. Denn im Falle des Revozierens eines Zertifikates sind außer im Verfahren des direkten Vertrauens immer weitere Zertifikate betroffen, so daß vor jeder Nutzung jedes in der Kette liegende Zertifikat überprüft werden müßte[351]. Diese Aufgabe kann eine Zertifizierungsstelle mittels eines Webservers lösen, wobei sekundengenaue Aktualität der Revozierungslisten jedoch nicht zu realisieren ist, oder dem Online-Zertifikatsstatusprotokoll.

Auf jeden Fall kann eine Zertifizierungsstelle Zertifikate ausgeben und die darin enthaltenen Informationen unter gewissen Voraussetzungen garantieren. Teilnehmer werden demnach automatisch allen anderen Teilnehmern der eigenen Zertifizierungsstelle vertrauen.

Da zum heutigen Zeitpunkt bereits mehrere Anbieter von Zertifikaten am Markt vertreten sind, müssen Regeln ähnlich den Vertrauensverfahren für Personen geschaffen werden, damit Teilnehmer einer Zertifizierungsstellen mit Teilnehmern einer anderen Zertifizierungsstelle sicher kommunizieren können.

Als erste Möglichkeit bietet sich wiederum das direkte Vertrauen an. In diesem Fall müßten sich jeweils zwei Zertifizierungsstellen gegenseitig zertifizieren[352]. Bei diesem Vorgang, Cross-Zertifizierung genannt, signiert jede Zertifizierungsstelle das Zertifikat der anderen, so daß Teilnehmer der einen die Zertifikate der Teilnehmer der anderen Zertifizierungsstelle überprüfen können[353]. Die Situation der Vertrauensverhältnisse wird durch Abbildung 4-5 verdeutlicht.

---

[351] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 146.

[352] Erläuterung am Beispiel einer Firmenübernahme in Barber (Implementing Public Key Infrastructures, 2000), S. 231.

[353] Vgl. Hammer (Cross-Zertifikate verbinden, 2001), S. 65.

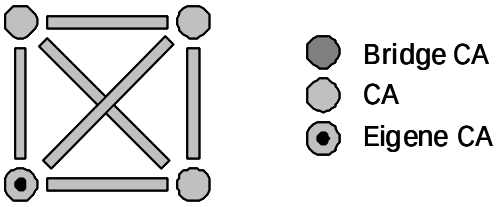

Abbildung 4-5 – Cross-Zertifizierung von Zertifizierungsstellen

Da es wenig wünschenswert ist, daß zwei beliebige Personen im Internet über ein Zertifikat verfügen, dieses aber nicht verifizieren können, müßten sich alle Zertifizierungsstellen gegenseitig zertifizieren, um direktes Vertrauen zu realisieren[354]. Eine Alternative wäre, Wege zuzulassen, so daß ähnlich dem Vertrauenverfahren von Personen ein Netz des Vertrauens entstünde. Aufgrund der geringeren Anzahl von Zertifizierungsstellen gegenüber Personen wäre die Zertifikatskettenlänge deutlich geringer, es bliebe jedoch die Problematik der Wege[355]. Außerdem dürfte die Verantwortung, eine neue Zertifizierungsstelle in das vorhandene Netz einzubeziehen, nicht von einer Zertifizierungsstelle alleine getroffen werden, da die Sicherheit des gesamten Netzes von der Sicherheit der schwächsten Stelle abhängt. Eine Darstellung dieser Situation findet sich in Abbildung 4-6.

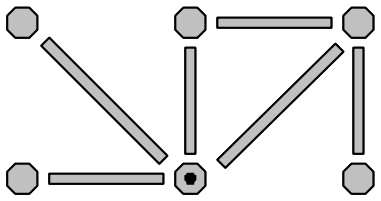

Abbildung 4-6 – Netz des Vertrauens mit Zertifizierungsstellen

Dieses Manko behebt die Struktur der Hierarchie[356], die unter anderem im Signaturgesetz vorgesehen ist[357]. Im Gegensatz zum Netz des Vertrauens werden zwei

---

[354] Vgl. Fox (Cross-Zertifikat, 2001), S. 105;
Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 146;
Vgl. Merz (Electronic Commerce, 1999), S. 139.

[355] Vgl. Hammer (Cross-Zertifikate verbinden, 2001), S. 68.

[356] Vgl. Perlman (An Overview of PKI Trust Models, 1999), S. 41.

Zertifizierungsstellen nicht cross-zertifiziert, sondern nur die in der Hierarchie höher stehende Zertifizierungsstelle zertifiziert die darunterliegende[358]. Die im Signaturgesetz beschriebene Struktur schränkt die Hierarchie auf zwei Stufen ein, das heißt, unter der Wurzelinstanz befinden sich Zertifizierungsstellen, die allesamt Teilnehmerzertifikate ausstellen. Dies sollte ausreichend sein, könnte doch mit einer Million Zertifikaten pro Zertifizierungsstelle, eine vom technischen Standpunkt aus betrachtet realistische Zahl, und bei Eintausend Zertifizierungsstellen eine Milliarde Zertifikate verwaltet werden. Problematisch könnte bei diesem Modell der Angriffspunkt der Wurzelinstanz (Single Point of Failure) sein[359], an der das komplette Modell hängt. Das hierarchische Modell, welches im Signaturgesetz Anwendung findet, ist in Abbildung 4-7 abgebildet.

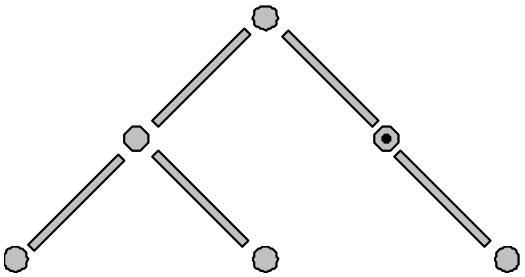

Abbildung 4-7 – Hierarchisches Modell

Außerdem könnte eingewandt werden, daß alle Teilnehmer einer Stelle vertrauen müssen. Während in Deutschland diese Funktion durchaus vom Staat übernommen werden könnte, ist dies in Ländern, in denen die Rolle des Staates weniger ausgeprägt ist, absolut undenkbar.

---

[357] Vgl. SigG §3;
Ausführlichere Erläuterungen finden sich in Camphausen/Kelm/Liedke/Weber (Aufbau und Betrieb einer Zertifizierungsinstanz, 2001), S. 29.

[358] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 134;
Vgl. Dusemund/Becker/Gollan/Engel/Meinel (The Functionality of a Public Key Infrastructure, 2000), S. 12.

[359] Vgl. RegTP (Elektronische Signaturen - FAQ, 2002), Frage 15.

Das vierte vorgestellte Vertrauensverfahren soll diese Problematik mit Hilfe einer Kombination aus Crosszertifizierung und Hierarchie lösen. Dies wird durch eine Zertifizierungsstelle erreicht, die zwei oder mehrere andere Zertifizierungsstellen cross-zertifiziert[360] und somit eine Brücke zwischen beiden bildet. Aus diesem Grund werden diese als Brückenzertifizierungsstellen (Bridge-Certification-Authorities) bezeichnet[361]. Zertifizierungsstellen schließen sich dabei einer oder mehreren Brückenzertifizierungsstellen an und ermöglichen damit ihren Teilnehmern mit allen anderen Teilnehmern der angeschlossenen Zertifizierungsstellen in Kontakt zu treten. Für jede Zertifizierungsstelle ist der Anschluß an eine oder mehrere Brückenzertifizierungsstellen möglich, da das Wurzelzertifikat nicht von der Brückenzertifizierungsstelle ausgestellt sondern lediglich cross-zertifiziert wird. Dadurch sind redundante Zertifikatsketten möglich, die im Interesse der Teilnehmer sind, aber organisatorisch berücksichtigt werden müssen. Außerdem könnten sich die Brückenzertifizierungsstellen gegeneinander durch unterschiedliche Sicherheitsniveaus abgrenzen oder mit identischen Leistungen im Service konkurrieren. Eine graphische Darstellung findet sich in Abbildung 4-8.

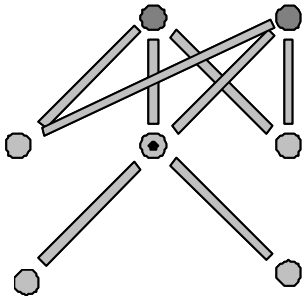

Abbildung 4-8 – Modell mit mehreren Brückenzertifizierungsstellen

[360] Vgl. Dusemund/Becker/Gollan/Engel/Meinel (The Functionality of a Public Key Infrastructure, 2000), S. 14.

[361] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 142;
Vgl. Esslinger/Barcklow/Bartosch (Global PKI and S/MIME Interoperability, 2001), S. 520;
Vgl. Deutsche Bank AG/Deutsche Telekom AG (Bridge-CA, 2001), Internet-Quelle;
Vgl. Reif (Bridge-CA, 2001), S. 553;
Vgl. Altmann (Federal Bridge Certification Authority, 2001), S. 687.

4.2 Klassifizierungskriterien für Zertifikate

Die Europäische Signaturrichtlinie zeigt einen Weg zur Entwicklung skalierbarer Lösungen auf, der für unterschiedliche Anwendungsfälle im öffentlichen Bereich und für den E-Commerce genutzt werden kann[362]. Hintergrund ist eine möglichst rasche Verbreitung elektronischer Signaturen im täglichen Leben und somit eine permanente Erhöhung der Sicherheit bezüglich der Kommunikation.

Eine Abstufung von verschiedenen Klassen für unterschiedliche Anwendungen ist aus mehreren Gründen sinnvoll. So kann der Anwender die Entscheidung über die von ihm benötigte Sicherheit selbst treffen[363]. Des weiteren läßt sich das Sicherheitsniveau jeder Klasse an das tatsächliche Gefährdungspotential anpassen[364]. Außerdem muß eine praktikable Lösung gefunden werden, um die Ziele Bedienbarkeit, Implementierbarkeit, ausreichendes Sicherheitsniveau und vernünftige Kosten möglichst optimal zu erfüllen[365]. In der IT-Sicherheit gibt es zahlreiche Beispiele für die Abstufung hinsichtlich der Sicherheitsrelevanz. Zertifizierungsinstrumente wie die ITSEC[366] oder CC[367] unterscheiden Sicherheitsstufen[368], die die Gefährdungslage, die Folgekosten eines Systemversagens oder eines Sicherheitsloches definieren. Ein weiteres Beispiel ist die Zugangs- oder Zugriffskontrolle in Unternehmen oder militärischen Einrichtungen. Sensible Dokumente oder Bereiche sollen nur berechtigten Personen zugänglich sein und je höher die Sicherheitsanforderungen eines Bereiches sind, um so höher dürfen die Kosten zur Ergreifung von Sicherheitsmaßnahmen sein. Eine Einteilung in Klassen hilft einer Kostenexplosion vorzubeugen, da nur besonders sensible Bereiche oder Dokumente mit dem

---

[362] Vgl. Welsch (Stufenweise skalierbare Sicherheit, 1999), S. 521.

[363] Vgl. Roßnagel (Europäische Signatur-Richtlinie, 1999), S. 265.

[364] Vgl. Fox (Zurück auf dem Boden, 2001), S. 442.

[365] Vgl. Schultz/Proctor/Lien/Salvendy (Usability and Security, 2001), S. 620ff.

[366] Eine Einteilung in Stufen E1 bis E6 erfolgt in Kapitel 4 der ITSEC. BSI (ITSEC, 2001), S. 45ff.

[367] Vgl. Common Criteria (Common Evaluation Methodology, 1999), Internet-Quelle.

[368] Vgl. Einen Vergleich bietet BSI (Vergleich CC - ITSEC, 2001), Internet-Quelle.

höchsten Aufwand geschützt werden[369]. Diese Einteilung sollte jedoch der Selbstregulierung des Marktes überlassen und nicht per Gesetz vorgegeben werden[370].
Die Entwicklung von Lösungen für hochsichere Anwendungen verursacht zudem erhebliche Entwicklungskosten, die sich amortisieren müssen. Dies läßt sich entweder durch einen hohen Preis oder eine hohe Stückzahl realisieren. Aber auch wenn sich die hochsichere Lösung durchaus in Bereichen einfacher Anwendungen einsetzen läßt, so bliebe trotzdem die Überlegung, ob nicht bei einem geringeren Preis eine größere Nachfrage entstünde. Diese schnellere Marktdurchdringung wiederum wäre eine entscheidende Voraussetzung für den Einsatz digitaler Signaturen im elektronischen Geschäftsverkehr[371]. Im folgenden werden Kriterien auf ihre Eignung zur Bildung dieser Einteilung von Sicherheitsklassen untersucht und der praktische und ökonomische Nutzen der resultierenden Klassen bewertet, die durch die Einteilung entstehen. Um nicht durch eine Vielzahl von Klassen das ohnehin komplexe Anwendungsgebiet weiter zu verkomplizieren, sind im Ergebnis wenige Klassen erwünscht, so daß genügend Spielraum zur Differenzierung geboten wird und trotzdem Übersichtlichkeit gewährleistet ist.
Als erstes wird eine Einteilung der Klassen im Hinblick auf die Rechtsverbindlichkeit der Kommunikation beschrieben. Da hier jeweils im einzelnen die Beweiskraft der Zertifikate zu prüfen ist, betrachtet ein zweiter Ansatz die Einteilung bezüglich der Beweiskraft der Zertifikate[372]. Als letztes wird eine Einteilung hinsichtlich des Kosten-Sicherheits-Verhältnisses vorgenommen, um die Klassenbildung zu erreichen.

---

[369] Vgl. Welsch (Stufenweise skalierbare Sicherheit, 1999), S. 521.

[370] Vgl. Rieß (Signaturgesetz - Der Markt ist unsicher, 2000), S. 534.

[371] Vgl. Welsch (Stufenweise skalierbare Sicherheit, 1999), S. 520.

[372] Vgl. Roßnagel (Europäische Signatur-Richtlinie, 1999), S. 265.

4.2.1 Rechtliche Anforderungen an die Formbedürftigkeit

Hinsichtlich der rechtlichen Anforderungen an die Kommunikation lassen sich 4 Stufen unterscheiden, die vom Bürgerlichen Gesetzbuch (BGB)[373] vorgesehen sind[374].

Als niedrigste Stufe S0, wird Authentifikation in Zusammenhang mit nicht rechtsverbindlicher Kommunikation gewählt. Da die Kommunikation nicht rechtsverbindlich ist, werden keine Anforderungen an das Verfahren gestellt. Einfachste Verfahren, beispielsweise PIN-Verfahren ohne zusätzliche Sicherheitsvorkehrungen wie der Besitz einer Chipkarte, reichen aus und können dementsprechend günstig umgesetzt werden.

Die nächst höhere Stufe S1 bildet Bereiche ab, in denen Verträge oder Willenserklärungen formfrei abgegeben werden können. Dieses System könnte auf Rechnern ohne Chipkartenlesegerät eingesetzt werden, da diese Lesegeräte zum heutigen Zeitpunkt noch nicht zur Standardausrüstung eines handelsüblichen Rechners gehören. Ein softwarebasiertes System, das auf Basis von Disketten, CDs oder Festplatten funktionieren müßte, hätte nicht die Beweiskraft eines dem Signaturgesetz entsprechenden Modells, würde aber trotzdem für zusätzliches Vertrauen sorgen. Ein solches Verfahren könnte niemals Beweissicherheit vor dem Gesetz erlangen, da der Gesetzgeber für diese Stufe keine technischen oder organisatorischen Vorschriften erlassen sollte. Denkbar wäre jedoch ein rechtlicher Rahmen, der beispielsweise durch freiwillige Akkreditierungs- oder Auditierungsverfahren ein gewisses Sicherheitsniveau schafft, das Anreiz wäre, diese Stufe zu verwenden. Letztendlich bliebe die kritische Würdigung des Beweiswertes einer Signatur jedoch der Rechtsprechung vorbehalten, die den Sicherheitswert im Laufe der Zeit ermitteln würde.

---

[373] Stufen finden sich beispielsweise in §126 Gesetzliche Schriftform oder §128 Notarielle Beurkundung.

[374] Sämtliche Stufen werden in Welsch (Stufenweise skalierbare Sicherheit, 1999) ab S. 524 erläutert.

Bei schriftformbedürftigen Willenserklärungen muß ein höheres Sicherheitsniveau erreicht werden, das Stufe S2 darstellt. Insbesondere muß die mit einer Unterschrift verbundene Warnfunktion gewährleistet werden[375]. Der Preis einer solchen Lösung läge über dem der Stufe S1[376], weshalb der Besitz eines Chipkartenlesegerätes ebenfalls vorausgesetzt werden kann. Diese bildet die Grundlage, um die notwendige Sicherheit für sensitive Anwendungen und Rechtsgeschäfte von besonderem Wert zu garantieren. Als Gegenwert für den höheren Kosten für einen Teilnehmer muß die Signatur der Stufe S2 daher über einen sicheren Beweiswert verfügen.

Als höchste Stufe S3 werden notariell zu beurkundende Dokumente eingeteilt[377]. Denkbar ist die Vorstellung, daß zwei Parteien zu jeweils einem anderen Notar gehen und beide Notare über das Internet gemeinsam für die rechtsverbindliche, notariell beglaubigte Urkunde sorgen. Die Vertragsparteien signieren dafür das Dokument online im Beisein ihres Notars, bevor beide Notare dies tun. Zu beachten ist, daß für diese Signatur auf jeden Fall Signaturen der Stufe S2 zu verwenden sind. Das Zusammentreffen zweier Personen an einem gemeinsamen Ort würde durch diese Prozedur entfallen. Die Anforderungen des Verfahrens gehen jedoch über die Signatur hinaus und betreffen zusätzlich den Prozeß der Beurkundung.

Als Ergebnis entstehen vier Klassen von Signaturen, von denen die niedrigste S0 an keine Bedingung geknüpft ist. Die Klassen S2 und S3 müssen vom Gesetz klar definiert werden, da die Beweiskraft garantiert werden muß. Die größte Klasse S1 ist lediglich begrenzt durch die Abhebung von S0 und das Fehlen einzelner Merkmale von S2.

---

[375] Vgl. Oertel (Elektronische Form und notarielle Aufgaben, 2001), S. 421.

[376] Zum einen resultieren daraus zusätzliche Anforderungen an die Software, mit der die Willenserklärungen abgegeben werden. Zum anderen kann dies nur mittels einer Chipkarte realisiert werden, deren Daten aus Sicherheitsgründen nicht ausgelesen werden können.

[377] Vgl. Oertel (Elektronische Form und notarielle Aufgaben, 2001), S. 422.

4.2.2 Beweiskraft der Signaturen

Obwohl das Kriterium der rechtlichen Anforderungen an die Formbedürftigkeit gewählt wurde, spiegelt das Ergebnis Klassen wieder, die sich im wesentlichen nach der Beweiskraft der Signatur richten. Dieser Ansatz ist sehr realitätsnah, weil jede Person selbst entscheiden kann, auf welche Art ein Vertrag geschlossen werden soll[378]. Für Geschäfte mit geringem Wert, beispielsweise der Kauf einer Zeitung, kann auf jegliche Sicherheit verzichtet werden, da der entstehende Aufwand die mit dem Geschäft verbundenen Risiken übersteigt. Im Gegensatz dazu wird bei Geschäften mit hohem Wert, von beiden Parteien Nachweisbarkeit gefordert werden.

Aus dem Blickwinkel des elektronischen Rechtsverkehrs sind demnach drei verschiedene Level der Regulierung und Administration von Signaturen zu unterscheiden, die unterschiedlichen Sicherheitsniveaus entsprechen[379].

Die niedrigste Stufe S0 entspräche einem Verfahren, bei dem mit Sicherheit keine Beweiskraft vorliegt. Solche Verfahren mit einem personenidentifizierenden Verfahren, zum Beispiel Pretty Good Privacy (PGP), ermöglichen eine Sicherung des Geschäftsverkehrs auf niedrigem Niveau.

Die nächst höhere Stufe S1 bietet keine Beweissicherheit, jedoch die Möglichkeit der Anerkennung vor Gericht[380]. Dadurch kann zwar einerseits keine Partei von der sicheren Beweisbarkeit ausgehen, andererseits aber auch nicht von der sicheren Abstreitbarkeit[381], so daß insgesamt eine deutlich höhere Sicherheit erreicht wird.

Das höchste anzunehmende Sicherheitsniveau entspricht der Stufe S2 mit Beweissicherheit. In diesem Fall muß der Gesetzgeber, wie er es durch das Signaturgesetz getan hat, für hohe und detaillierte Anforderungen sorgen, die insgesamt ein ho-

---

[378] Vgl. Welsch (Stufenweise skalierbare Sicherheit, 1999), S. 521.

[379] Vgl. Roßnagel (Europäische Signatur-Richtlinie, 1999), S. 265.

[380] Vgl. Roßnagel (Das neue Signaturgesetz, 2001), S. 202.

[381] Wenn ein Gericht die Signatur als Beweis anerkennt, kann diese nicht mehr bestritten werden. Für die freie Beweiswürdigung des Gerichts siehe Kuner (Signaturgesetz und "Political Correctness", 1999), S. 227.

hes Maß an Sicherheit gewährleisten. Durch eine Vorabprüfung der Einrichtung und eine Genehmigungspflicht erhalten sie eine Sicherheitsvermutung, die den höheren Aufwand und die damit verbundenen höheren Kosten rechtfertigen. Durch die Möglichkeit der Bundesrepublik Deutschland, in öffentlichen Bereichen dieses Sicherheitsniveau festzuschreiben, kann diese Stufe ein breites Anwendungsfeld erhalten[382]. Inwiefern diese Annahme realistisch ist, bleibt abzuwarten. Ebenso wahrscheinlich ist ein vollständiger Verzicht auf diese Stufe, da Kosten und Nutzen aufgrund des engen Anwendungsgebietes in keinem Verhältnis stehen.

4.2.3 Kosten-Sicherheits-Verhältnis

Obwohl beide vorher genannten Kriterien die Kosten der Zertifikate implizit berücksichtigen, fehlt der konsequente Bezug zwischen den Kosten und dem damit erreichten Sicherheitsniveau. Denn die Frage ist nicht, ob durch höhere Kosten mehr Sicherheit erreicht werden kann, sondern mit wieviel zusätzlichen Kosten welcher Zugewinn an Sicherheit realisiert werden kann[383].

[382] Vgl. Roßnagel (Europäische Signatur-Richtlinie, 1999), S. 265.

[383] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 1.2.

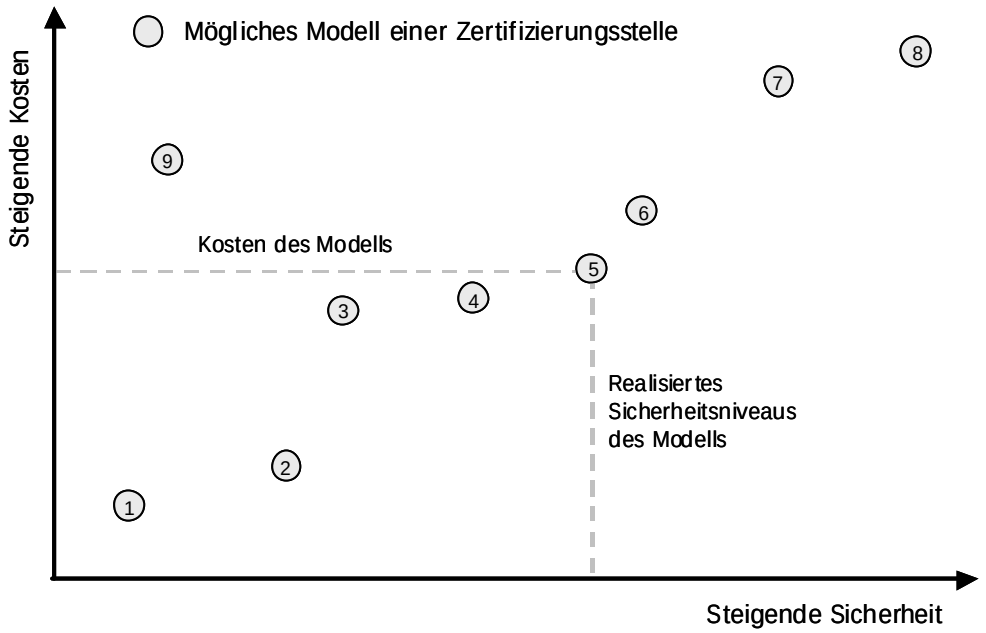

Abbildung 4-9 – Modelle nach Kosten und Sicherheitsniveau

In Abbildung 4-9 sind neun mögliche Modelle für Zertifizierungsstellen eingezeichnet, die sich hinsichtlich des erreichten Sicherheitsniveaus und der zur Realisierung angefallenen Kosten unterscheiden. Die zu bildenden Klassen sollen nun nicht durch Kriterien wie Formbedürftigkeit oder Beweisbarkeit bestimmt werden, sondern durch das Kosten-Sicherheits-Verhältnis der Zertifizierungsstellen und damit der ausgestellten Zertifikate.

Erwähnenswert sind die im allgemeinen nicht proportional sondern überproportional mit dem Sicherheitsniveau ansteigenden Kosten[384]. Daher bietet sich eine logarithmische Kostenachse mit entsprechend hohen Kostenunterschieden in den oberen Bereichen der Abbildung an.

Die Sicherheit eines zu beurteilenden Systems richtet sich entsprechend nach der höchsten realisierten Maßnahme, die direkt vor der ersten nicht realisierten genannt wird. Dabei kann es vorkommen, daß Modelle aufgrund von Sicherheitsmängeln in einzelnen Teilbereichen über ein ungünstiges Kosten-Sicherheits-Verhältnis verfügen. Im Beispiel kann daher Modell 9 von der Betrachtung ausge-

[384] Vgl. Raepple (Sicherheitskonzepte für das Internet, 2001), S. 9.

schlossen werden, da Modell 2 ein höheres Sicherheitsniveau zu geringeren Kosten realisiert und daher zu präferieren ist.

Um aus dem Kosten-Sicherheits-Verhältnis direkt Sicherheitsklassen bilden zu können, ist im ersten Schritt ein Referenzmodell auszuwählen. Im Falle der Zertifizierungsstellen definiert der Gesetzgeber eine obere Grenze, ab der Beweissicherheit gilt. In der folgenden Abbildung soll Modell 8 die Anforderungen dieser Grenze erfüllen. Dieses Modell wird als Referenzmodell bezüglich des Kosten-Sicherheits-Verhältnisses ausgewählt, das durch die gestrichelte Gerade dargestellt wird. Jedes Modell auf dieser Linie verfügt über das gleiche Kosten-Sicherheits-Verhältnis. Modelle auf konvexen Teilabschnitten und vergleichsweise günstigerem Kosten-Sicherheits-Verhältnis realisieren ein Sicherheitsniveau zu relativ gesehen niedrigeren Kosten und sind daher den anderen Modellen vorzuziehen[385]. Jedes dieser Modelle könnte als Grenze einer Klasse dienen, wobei diese jedoch über einen gewissen horizontalen Abstand verfügen sollten, da der Nutzen der Klasseneinteilung ansonsten fragwürdig ist. Im Falle zu vieler Klassen, können Modelle bei der Klassenbildung ausgelassen, bei zu wenigen Klassen können zusätzlich Modelle hinzugenommen werden, selbst wenn das dazugehörige Kosten-Sicherheits-Verhältnis nicht optimal ist[386]. Die Anzahl der Klassen sollte drei bis fünf nicht übersteigen, damit die Übersichtlichkeit und Unterscheidbarkeit gewährleistet bleibt. Eine Weiterentwicklung von Abbildung 4-9 nach den geschilderten Regeln findet sich in Abbildung 4-10, bei der die resultierenden Sicherheitsklassen eingezeichnet sind.

[385] Im Beispiel Modelle 2 und 5.

[386] Im Beispiel Modelle 1, 4 und 6.

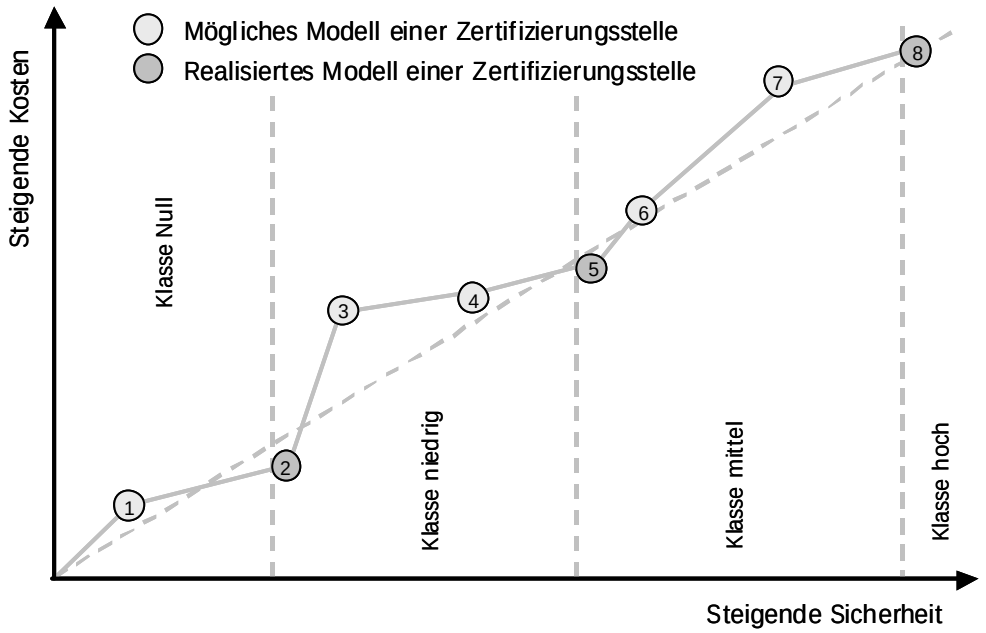

Abbildung 4-10 – Sicherheitsklassen nach dem Kosten-Sicherheits-Verhältnis

Die Klassen werden in dem betrachteten Umfeld durch die Modelle 2, 5 und 8 bestimmt und schließen jeweils alle anderen Modelle ein, die ein höheres Sicherheitsniveau als sie selbst, aber ein geringeres als die nächst höhere Klasse bieten. Zusätzlich existiert die Klasse Null, die nur Modell 1 einschließt und keine Sicherheit symbolisiert. Dies wird deutlich, wenn ein Modell 0 in die Überlegungen einbezogen wird, das keine Kosten zur Erhöhung der Sicherheit akzeptiert. Dieses befindet sich im Ursprung des Graphen und bildet damit die Klasse Null. In der niedrigsten Sicherheitsklasse der nach dem Kosten-Sicherheits-Verhältnis definierten Klasseneinteilung befinden sich die Modelle 2, 3 und 4, in der mittleren Klasse die Modelle 5, 6 und 7 und in der höchsten Klasse nur das Modell 8.

Müssen mehrere Kosten-Sicherheits-Verhältnisse unterschiedlicher Teilaspekte einer Gesamtbetrachtung in Einklang gebracht werden, so sind zwei Fälle denkbar. Im einfachen Fall stimmen die gefundenen Stufen hinsichtlich der Anzahl und des erreichten Sicherheitsniveaus überein, und somit kann das Gesamtergebnis direkt aus der Kombination der Klasseneinteilungen der Teilaspekte gebildet werden.

Im anderen Fall können mehrere Unterschiede vorliegen, die hintereinander untersucht und behoben werden müssen. Zunächst können in den einzelnen Teilaspek-

ten eine unterschiedliche Anzahl an Klassen existieren, die einen Vergleich der Klassen verhindert. Durch die Einführung zusätzlicher Klassen, die mittels unterschiedlicher Modelle oder die doppelte Nutzung eines Modells für zwei oder mehr Klassen erreicht werden kann, wird die Klassenzahl in Teilaspekten mit weniger Klassen erhöht. Verdeutlicht wird dieser Tatbestand durch die Abbildung 4-11, bei der entweder eines der Modelle 3 bis 5 zur Bildung einer neuen Klasse oder Modell 6 zusätzlich für die mittlere Klasse verwendet werden kann. Dafür spräche, daß den geringen Mehrkosten ein wesentlich größerer Sicherheitsgewinn gegenüberstehen würde.

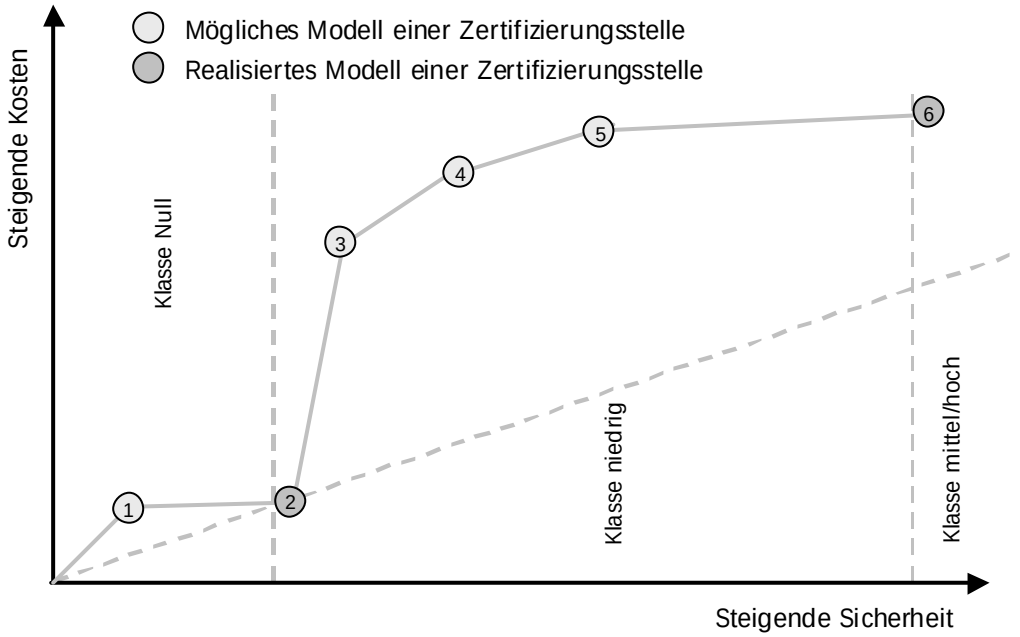

Abbildung 4-11 – Doppelnutzung eines Modells für zwei Klassen

In Teilaspekten mit zu vielen Klassen kann das Angleichen der Klassenzahl durch die Entfernung von Klassen realisiert werden. Außerdem können differierende Sicherheitsniveaus der resultierenden Klassen vorliegen. Dabei müssen deutliche Unterschiede verhindert werden, weil sich die Sicherheit identischer Klassen mit unterschiedlichen Sicherheitsniveaus nach dem niedrigsten Sicherheitsniveau aller betrachteten Teilaspekte richtet. Die Gesamtsicherheit eines Systems ist immer

nur so stark wie der schwächste Teil[387]. Im Interesse des Gesamtsystems kann deshalb eine Verschiebung einer Klasse innerhalb eines Teilaspektes auf ein nach dem Kosten-Sicherheits-Verhältnis ungünstigeres Modell im Gesamtergebnis Vorteile gegenüber dem reduzierten Sicherheitsniveau bieten. Dies wird in Abbildung 4-12 verdeutlicht, indem durch die Verwendung von Modell 3 zur Klassenbildung, das Sicherheitsniveau der mittleren Klasse des Gesamtsystems auf das von Teilaspekt 2 angehoben würde. Zu beachten ist jedoch, daß dies nur gilt, wenn der betrachtete Teilaspekt nicht der mit Abstand kostenintensivste ist.

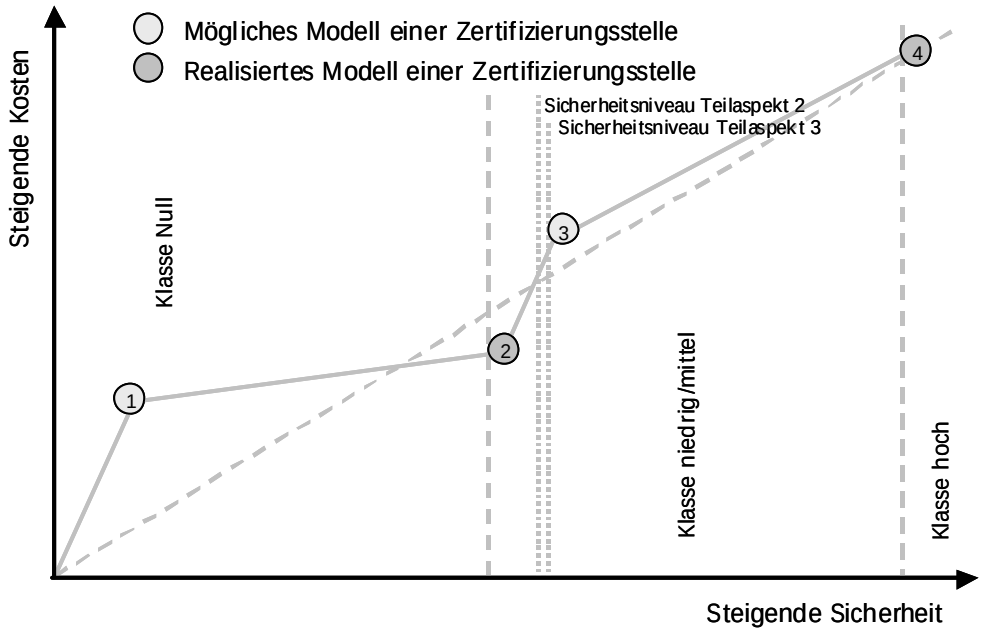

Abbildung 4-12 – Suboptimale Klassenverschiebung innerhalb eines Teilaspektes

In der Praxis können mit diesem Vorgehen verschiedene Sicherheitsniveaus gebildet werden, die zum einen vergleichbar sind und zum anderen einen klaren Bezug zu den entstehenden Kosten aufweisen. Der Anwender erhält die Möglichkeit, das Sicherheitsniveau dem Gefährdungspotential anzupassen, indem er die Kosten eventueller Schadenszenarien den Kosten potentieller Sicherheitsniveaus gegen-

[387] Vgl. Schneier (Secrets & Lies, 2001), S. 359.

überstellt. Als Ergebnis ergibt sich ein pragmatischer Ansatz, der sich bislang bei allen Einführungen von neuen Technologien bewährt hat[388].

4.3 Prozesse der Zertifizierungsstellen

In den folgenden Abschnitten sollen die Prozesse einer Zertifizierungsstelle untersucht werden, die den Teilnehmern in Rechnung gestellt werden oder gestellt werden könnten. Aus diesem Grund werden die Gemeinkosten, zum Beispiel das Gebäude, die Instandhaltung oder Bewachung des Gebäudes oder Datensicherungsmaßnahmen, nicht betrachtet. Sie fallen unabhängig von den Prozessen an und werden nur durch andere Faktoren, beispielsweise Sicherheit, beeinflußt. Für den Teilnehmer sind sie nicht sichtbar und nicht von Relevanz, sofern die geschilderten Prozesse nicht behindert werden oder nicht mehr geleistet werden können.
Mit dem Kauf eines Zertifikates oder dem Wunsch eines Zeitstempels tritt ein Teilnehmer mit einer Zertifizierungsstelle in Kontakt und löst einen Prozeß aus, der auf Seiten der Zertifizierungsstelle Kosten verursacht. Die dabei für den Teilnehmer entstehenden Kosten müssen vom entstehenden Nutzen des Teilnehmers aufgewogen werden, da er ansonsten von der Nutzung absehen wird. Das bedeutet, daß die Kosten der Zertifizierungsstelle für die einzelnen Prozesse diesen Betrag nicht überschreiten dürfen, da es ansonsten günstiger wäre, den Verkauf einzustellen. Das Insolvenzverfahren der Zertifizierungsstelle liegt keinesfalls im Interesse des Teilnehmers, da er auf die kontinuierliche Dienstleistung angewiesen ist.
Begonnen wird daher mit dem ursprünglichen Prozeß der Ausstellung eines Zertifikates, bevor die Sperrung und Prüfung betrachtet wird. Danach werden der Zeitstempeldienst und die Prüfung eines Zeitstempels betrachtet, bevor zuletzt die Rechnungsstellung untersucht wird[389]. Eine graphische Übersicht der Prozesse finden Sie in Abbildung 4-13.

---

[388] Vgl. Welsch (Stufenweise skalierbare Sicherheit, 1999), S. 521.

[389] Vgl. Adams/Lloyd (Understanding Public-Key-Infrastructure, 1999), S. 33ff;
Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 4-5.

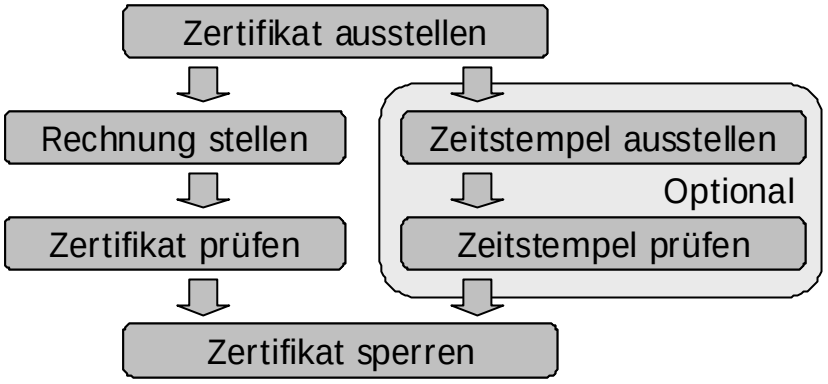

Abbildung 4-13 – Übersicht der Prozesse einer Zertifizierungsstelle

4.3.1 Ausstellung von Zertifikaten

Die Ausstellung eines Zertifikates stellt den aufwendigsten Prozeß einer Zertifizierungsstelle dar. Neben der Teilnehmeridentifizierung und –registrierung müssen eventuell Schlüssel für den Teilnehmer erzeugt, ein Zertifikat erstellt und das Trägermedium personalisiert werden[390].

Der wichtigste Vorgang bei der Ausstellung eines Zertifikates ist die Identifikation des Teilnehmers, da dieser mit dem Zertifikat in der Lage ist im Rechtsverkehr unter der Identität des Zertifikatsinhabers aufzutreten[391]. Am schnellsten kann dieser Prozeß ablaufen, wenn der Teilnehmer persönlich bei der Zertifizierungsstelle erscheint. Er kann in der Aufnahme seinen Antrag abgeben, der sofort geprüft wird und erhält kurze Zeit später in der Ausgabe sein personalisiertes Trägermedium, mit dem er digitale Unterschriften leisten kann. Da nicht jeder Teilnehmer in unmittelbarer Nähe zur Zertifizierungsstelle wohnt, kann ein persönliches Erscheinen unter Umständen mit einem hohen Zeitaufwand verbunden sein. Aus diesem Grund muß der gesamte Prozeß zusätzlich auf dem Postweg abgebildet werden. In diesem Fall trifft der Antrag schriftlich ein, wobei die Identifizierung

[390] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 4.

[391] Vgl. Harnier (Organisationsmöglichkeiten für Zertifizierungsstellen, 2000), S. 76.

des Teilnehmers von Dritten[392] bereits durchgeführt wurde. Nach der Bearbeitung geht dem Teilnehmer das Trägermedium und in getrennter Post die Zugangskennung des Benutzer-Authentifizierungsverfahrens zu. Der Erhalt beider Pakete muß vom Empfänger bestätigt werden und erst nach Prüfung der Bestätigung ist das Zertifikat gültig.

Zusätzlich muß eine Möglichkeit geschaffen werden, die es dem Teilnehmer ermöglicht, sich telefonisch zu authentifizieren, um sein Zertifikat sperren zu lassen. Dies könnte beispielsweise über eine zusätzliche PIN oder ein Paßwort erfolgen. Zum Abschluß des Prozesses muß das Zertifikat im Verzeichnisdienst bereitgestellt werden und eine Abrechnung der geleisteten Dienste gegenüber dem Teilnehmer erfolgen.

4.3.2 Sperrung von Zertifikaten

Die Sperrung einer Zertifikates ist notwendig, wenn ein Teilnehmer sein Trägermedium verliert oder den Verdacht hat, sein Zertifikat sei kompromittiert worden. In diesem Fall muß er sein Zertifikat schnellstmöglichst sperren lassen, um Mißbrauch zu verhindern. Der Prozeß der Sperrung von Zertifikaten ist nicht zu verwechseln mit dem normalen Ablauf des Gültigkeitszeitraum eines Zertifikates.

Im Gegensatz zur Ausstellung von Zertifikaten handelt es sich bei der Sperrung um einen zeitkritischen Prozeß, bei dem die Prozeßlaufzeiten eine wichtige Rolle spielen.

Die Zertifizierungsstelle muß über ein Call-Center verfügen, bei dem jeder Teilnehmer jederzeit anrufen kann, um sein Zertifikat zu sperren. Die Kapazität des Call-Centers muß ausreichend kalkuliert sein, damit kein Teilnehmer in der Warteschlange verweilen muß, bevor er sein Zertifikat sperren lassen kann. Ansonsten könnte die Zertifizierungsstelle für eventuellen Mißbrauch des Zertifikates haftbar gemacht werden[393]. Ob auf die Einrichtung eines eigenen Call-Centers aus Kosten-

---

[392] Dies könnte beispielsweise durch das Post-Ident-Verfahren der Deutschen Post erfolgen. Vgl. Deutsche Post (Post-Ident 3, 2001), Internet-Quelle.

[393] Vgl. Kapitel 4.4.1.

gründen verzichtet werden muß, wird in Kapitel 5.3.1 näher betrachtet, da die Einrichtung mit hohen Investitionen verbunden ist[394] und die Dienste der Sperrung von anderen Mitarbeitern übernommen werden könnten.

Neben dem sofortigen Vermerk der Sperrung des Zertifikates muß es bei der Erstellung der nächsten Revozierungsliste berücksichtigt werden[395]. Bis zur Veröffentlichung dieser Liste vergeht ein längerer Zeitraum, der von dem Zeitpunkt der letzten Veröffentlichung einer Revozierungsliste abhängt, da diese Veröffentlichungen in regelmäßigen Zeitabständen durchgeführt werden[396]. Dies bedeutet für Teilnehmer, die auf die Onlineüberprüfung von Zertifikaten verzichten und sich statt dessen auf die Revozierungslisten verlassen, einen Unsicherheitszeitraum. Erst mit der folgenden Revozierungsliste, auf dem das zu überprüfende Zertifikat nicht aufgeführt ist, ist die Gültigkeit des Zertifikates bestätigt, da die Sperrung des Zertifikates zwischen der Veröffentlichung der Revozierungsliste und dem Zeitpunkt der Überprüfung gelegen haben könnte.

Für die Zertifizierungsstelle resultiert aus diesen Gegebenheiten ein beträchtliches Haftungsrisiko, da bereits bei einer Verzögerung des Sperrprozesses[397] und gleichzeitigem Mißbrauch der Schaden eines Teilnehmers auf die Zertifizierungsstelle übertragen werden kann. Insbesondere könnte ein bewußtes Herbeiführen dieser Konstellation von Angreifern ausgenutzt werden.

Die Kosten für die Sperrung eines Zertifikates sollten in den Kosten der Ausstellung des Zertifikates enthalten sein, so daß hier für den Teilnehmer keine zusätzlichen Kosten außer den eigenen Telefongebühren anfallen. Die Kosten für das Call-Center müssen damit vollständig auf die ausgegebenen Zertifikate umgelegt werden. Gegebenenfalls kann die Zertifizierungsstelle bei der Kalkulation davon ausgehen, daß nicht alle Zertifikate, sondern nur ein Teil der ausgegebenen Zertifikate gesperrt wird. Dies führt zu einer entsprechenden Reduzierung der Kosten eines

---

[394] Vgl. o.V. (Investitionskosten beim Aufbau eines Call Centers, 2001), S. 1ff.

[395] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 5;
Vgl. Stark/Biester/Fell/Volk u.a. (PKI Organisationshandbuch, 2001), S. 45.

[396] Vgl. Fox (Certification Revocation List (CRL), 2001), S. 485.

[397] Vgl. Kapitel 3.2.1, Abschnitt Sperrmanagement.

Zertifikates, hat jedoch das Risiko zur Folge, daß mehr als der veranschlagte Teil der Teilnehmerzertifikate gesperrt werden.

4.3.3 Prüfung von Zertifikaten

Der Prozeß des Prüfens eines Zertifikates muß vollständig elektronisch abgebildet sein. Zunächst muß die Signatur mit Hilfe des öffentlichen Schlüssels der Zertifizierungsstelle geprüft werden. Handelt es sich um ein gültiges Zertifikat, bei dem der Gültigkeitszeitraum noch nicht abgelaufen ist, muß in der aktuellsten Revozierungsliste kontrolliert werden, ob zwischenzeitlich eine Sperrung vorgenommen wurde. In bestimmten Fällen können aktuellere Informationen über den Zustand des Zertifikates erwünscht sein, so daß eine online Überprüfbarkeit der Sperrung möglich sein muß. Durch die automatische Realisierung des Prozesses werden hier die geringsten Kosten pro Prüfung anfallen, die für den Teilnehmer ebenfalls bereits im Preis des Zertifikates enthalten sein sollten.

4.3.4 Dokument mit Zeitstempel versehen

Ein Prozeß, den eine Zertifizierungsstelle nicht selbst anbieten muß, aber zum Beispiel bei der Ausstellung eines Zertifikates benötigt wird, ist der des Verbindens eines Dokumentes mit der aktuellen Zeit[398], die Erstellung eines Zeitstempels. Dabei ist lediglich die Uhrzeit im Klartext mit dem Hashwert des gewünschten Dokumentes von der Zertifizierungsstelle zu signieren, so daß durch die Verifikation der Signatur der Zeitpunkt bestätigt wird. Aus diesem Grund handelt es sich um einen einfachen, ebenfalls vollständig automatisierbaren Prozeß.

Sofern der Prozeß allerdings extern angeboten wird, muß eine zusätzliche Authentifizierung der Nutzer eingeführt werden, um die geleisteten Dienste abrechnen zu können. Problematisch bei der Abrechnung sind die geringen Kosten und der geringe Nutzen eines Zeitstempels, die nur einen entsprechend geringen Marktpreis ermöglichen. Im Gegensatz dazu stehen die verhältnismäßig hohen Kosten der Rechnungsstellung, die eine Einzelabrechnung unter wirtschaftlichen Kriterien

---

[398] Vgl. Görg/Meinel/Engel (Konzeption einer Zertifizierungsstelle, 1997), S. 5.

verhindert. Hier gilt es, eventuell attraktive Pakete für Klein- und Großabnehmer anzubieten, von einer externen Bereitstellung des Dienstes abzusehen oder diesen nur in Verbindung mit einem Zertifikat anzubieten[399].

4.3.5 Prüfung von Zeitstempeln

Die Prüfung entspricht der Gültigkeitsprüfung eines Zertifikates, da nur die Signatur des Zeitstempels überprüft werden muß. Der Teilnehmer muß zusätzlich den Hashwert des Dokumentes überprüfen, dies erfolgt jedoch unabhängig von der Zertifizierungsstelle.

Die Kosten der Prüfung eines Zeitstempels liegen damit unter denen der Prüfung eines Zertifikates. Wie bereits weiter oben ausgeführt, sind diese aufgrund der vollständigen Automatisierbarkeit des Prozesses als gering einzustufen. Des weiteren sollten ebenfalls im Preis des Zeitstempels enthalten sein, den der Teilnehmer entrichten muß.

4.3.6 Rechnungsstellung

Der Prozeß der Rechnungsstellung wird an dieser Stelle untersucht, da dieser mit erheblichen Kosten[400] verbunden ist und für den Kunden sichtbar ist. Alle mit der Rechnungsstellung verbundenen Kosten sollten in den in den Preisen der Produkte enthalten sein, beziehungsweise auf die vorher genannten Prozesse, für die die Rechnungen gestellt werden, umgelegt werden.

Die Zertifizierungsstelle muß sämtliche abzurechnenden Dienstleistungen dem Kunden in Rechnung stellen und die Rechnung dem Kunden per Post oder in elektronischer Form übermitteln. Sofern kein Lastschriftauftrag vorliegt, muß der Zahlungseingang des Teilnehmers kontrolliert werden. In beiden Fällen ist eventuell ein Mahnverfahren einzuleiten, um fällige Zahlungen einzutreiben.

---

[399] Auf diese Art verfährt die Deutsche Telekom AG, siehe Deutsche Telekom AG (Public Key Service Informationen, 2001), S. 10.

[400] Die Deutsche Post Com schätzt die Kosten auf 7-15 DM (3,58-7,67 €) in Westermann (Neuer eBusiness-Service, 2000), S. 1.

4.4 Klassifizierung der Angriffe auf Zertifizierungsstellen

Um einschätzen zu können, welche Vor- und Nachteile die entsprechenden Modelle hinsichtlich der Sicherheit der ausgegebenen Zertifikate bieten, müssen die vorhandenen Risiken näher untersucht werden. Hierbei soll es zunächst nicht um die konkreten Risiken, das heißt die Wahrscheinlichkeiten und Schadenausmaße einzelner Unfälle, sondern um die prinzipiellen Risiken einer Zertifizierungsstelle gehen.

Aus Sicht der Zertifizierungsstelle müssen fünf Fälle der Kompromittierung von Zertifikaten unterschieden werden, die sich im wesentlichen durch die Anzahl der kompromittierten Zertifikate unterscheiden und in jeweils eigenen Kapiteln betrachtet werden. Die geringst mögliche Anzahl, genau ein Zertifikat, stellt den ersten Fall dar, wobei es sich um das Zertifikat eines Teilnehmers und keiner Zertifizierungsstelle handeln soll. Dieser wird im ersten Kapitel erläutert. Im folgenden Kapitel wird beschrieben, wie sich der Sachverhalt darstellt, wenn es sich dagegen um mehrere Zertifikate handelt, so daß der Schaden ungefähr proportional zur Anzahl der kompromittierten Zertifikate steigen kann. Im dritten Fall wird ein Zertifikat einer Zertifizierungsstelle kompromittiert, so daß implizit weitere Zertifikate, deren Gültigkeit darauf beruhen, ungültig werden[401]. Das Schadenausmaß richtet sich nach Einsatz des Vertrauensmodells und Bedeutung der Zertifizierungsstelle. Im vierten und fünften Kapitel werden die Fälle beschrieben, bei denen nicht mehr Zertifikate sondern Verfahren kompromittiert werden. Sollte ein eingesetztes Verfahren unsicher werden, so werden damit gleichzeitig alle Zertifikate ungültig, die auf diesem Verfahren beruhen. Insbesondere bei diesem Fall spielt die Verbreitung des Verfahrens eine wichtige Rolle bei der Beurteilung des Schadens. Im folgenden soll im fünften Kapitel der Fall betrachtet werden, bei dem alle eingesetzten Verfahren zur gleichen Zeit kompromittiert werden. Dieser stellt mit Sicherheit den größten anzunehmenden Unfall dar. Im sechsten und

[401] Vgl. Hammer (Cross-Zertifikate verbinden, 2001), S. 68.

letzten Kapitel werden Angriffe gegen die Verfügbarkeit der Dienstleistungen der Zertifizierungsstelle untersucht.

4.4.1 Kompromittierung eines Teilnehmerzertifikates

Durch die Kompromittierung eines Teilnehmerzertifikates sind die geringsten Auswirkungen der betrachteten Fälle zu befürchten. Nichtsdestotrotz liegt eine beachtliche Spanne möglicher Schadensfälle vor.

Im folgenden wird davon ausgegangen, daß ein Angreifer, der in den Besitz einer Chipkarte mit einem privaten Schlüssel gekommen ist, diese nach einer bestimmten Zeitspanne verwenden und damit die Identität des Besitzers annehmen kann.

Im Fall des Verlustes oder Diebstahls einer Chipkarte muß nach der Zeitspanne unterschieden werden, die der rechtmäßige Besitzer bis zum Erkennen des Verlustes benötigt[402]. Bemerkt dieser den Verlust innerhalb des Zeitrahmens, den ein Angreifer benötigt, um die gestohlene Karte verwenden zu können, kann durch eine Sperrung des Zertifikates ein Schaden vermieden werden. Hierbei ist jedoch zu berücksichtigen, daß die benötigte Zeit des Angreifers nicht feststeht, da dieser zum Zeitpunkt des Diebstahls schon im Besitz der notwendigen Kenntnisse sein könnte. Des weiteren müssen die Prozeßlaufzeiten der Zertifizierungsstelle berücksichtigt werden, die Zeit, die zwischen dem Anruf des sperrenden Teilnehmers und der tatsächlichen Sperrung des Zertifikates liegt. Inklusive der Zeit zur Authentifizierung des Anrufers bis zur Sperrung des Zertifikates auf dem Server sollten nicht mehr als 10 Minuten vergehen[403]. Aus diesem Grund ist der Sperrzeitpunkt zu vermerken[404]. Zuletzt sind noch die Intervalle der Veröffentlichung der Revozierungslisten zu berücksichtigen, da nicht für jeden Geschäftsvorfall online bei der Zertifizierungsstelle nachgefragt werden muß. Sollte der Verlust der Karte nicht erkannt werden können, da der Angreifer beispielsweise in den Besitz einer Kopie gelangt ist, so wird der Verlust erst beim erstmaligen Mißbrauch feststellbar sein.

---

[402] Erläuterungen dazu finden sich im Kapitel 3.2.1 im Absatz Sperrmanagement.

[403] Vgl. Bertsch/Pordesch (Problematik von Prozeßlaufzeiten, 1999), S. 514ff.

[404] Vgl. Blum (Entwurf eines neuen Signaturgesetzes, 2001), S. 73.

Ein weiteres Merkmal zur Unterscheidung des Schadens ist das Zertifikat an sich, da hier Einschränkungen vorgenommen werden können. Dies kann zum Beispiel ein Maximalbetrag sein, der die Gültigkeit des Zertifikates einschränkt.
Im Falle eines kompromittierten Teilnehmerzertifikates muß, neben der eventuellen Behebung des Schadens, die Zertifizierungsstelle dem Teilnehmer ein neues Zertifikat ausstellen. Da der Teilnehmer seine Identität nicht mehr elektronisch nachweisen kann, kann der Empfang der Smart-Card mit seinem neuen privaten Schlüssel nicht elektronisch bestätigt werden. Der Aufwand ist demnach höher als die Verlängerung eines noch gültigen Zertifikates, aber niedriger als eine reguläre Neuausstellung.

4.4.2 Kompromittierung mehrerer Teilnehmerzertifikate

Aufgrund des möglicherweise geringen Nutzens eines einzelnen Teilnehmerzertifikates könnten Angreifer gleich mehrere Zertifikate mißbrauchen. Anders als bei heutigen Kreditkarten, bei denen beispielsweise beim Bezahlen Angestellte eine Geschäftes leicht eine Kopie der Daten der Karte anfertigen können, funktioniert dies bei Zertifikaten nicht, zumindest nach dem heutigen Stand des Wissens[405]. Ein denkbarer Fall wäre jedoch der Mißbrauch durch Mitarbeiter der Zertifizierungsstelle, weshalb an diese besondere Ansprüche hinsichtlich des Vertrauens gestellt werden. Ebenso möglich wären Fehler bei der Erstellung oder Verteilung der Revozierungslisten, so daß Zertifikate trotz Sperrung noch benutzt werden könnten[406].
Da es sich bei diesem Szenario um eine beliebige Anzahl einzelner Kompromittierungen eines Zertifikates handelt, verhält sich der Aufwand proportional zu der eines einzigen Zertifikats. Jeder Teilnehmer bräuchte ein neues Zertifikat und muß dieses von der Zertifizierungsstelle ausgestellt bekommen. Der Aufwand zur Ausstellung neuer Zertifikate kann analog des Einzelfalls beurteilt werden.

---

[405] Vgl. Hammer (Die 2. Dimension der IT-Sicherheit, 1999), S. 77;
Vgl. SecCommerce (Smartcards: Physikalische Sicherheit, 2001), Internet-Quelle.

[406] Vgl. Mack (Sperren von Zertifikaten, 2001), S. 465.

4.4.3 Kompromittierung des Wurzelzertifikates

Neben einem Unfall innerhalb der Zertifizierungsstelle aufgrund dessen das Wurzelzertifikat veröffentlich wird, sind Angriffe beziehungsweise Einbrüche denkbar, die an der Sicherheit des Zertifikates zweifeln lassen und damit einen Austausch erzwingen würden. Unwahrscheinlich, aber nicht unmöglich, wäre glückliches Raten eines Angreifers, der zwar auf keinen Fall alle möglichen Schlüssel ausprobieren kann, vielleicht aber per Zufall den richtigen. Zwar ist es wesentlich wahrscheinlicher den wöchentlichen Lotto-Jackpot zu gewinnen, aber aus Sicht der Zertifizierungsstelle trotzdem ein zu berücksichtigendes Ereignis[407].

Der geringeren Eintrittwahrscheinlichkeit der Angriffe steht ein höheres Schadenspotential gegenüber. Alle Zertifikate, die mit diesem Zertifikat signiert worden wären, verlören zu diesem Zeitpunkt ihre Gültigkeit, da diese auf der mittels diesem Zertifikat erstellten Signatur der Zertifizierungsstelle beruht[408]. Dies trifft zum einen die Nutzer der Zertifizierungsstelle, zum anderen aber eventuell andere Zertifizierungsstellen. Nach dem Signaturgesetz wären nach einer Kompromittierung des Wurzelzertifikates der Regulierungsbehörde für Telekommunikation und Post (RegTP) alle ausgestellten qualifizierten Zertifikate ungültig[409]. Zunächst müßten demnach alle angeschlossenen Zertifizierungsstellen neue Zertifikate erhalten, bevor diese ihrerseits mit dem Ausstellen neuer Zertifikate beginnen könnten.

Im Falle des Ungültigwerdens aller Zertifikate einer Zertifizierungsstelle stellt sich dieser zusätzlich zur reinen Neuausstellung ein logistisches Problem der Abwicklung. Handelt es sich um eine Zertifizierungsstelle, die beispielsweise 150.000 Zertifikate im Umlauf hat, entspricht dies bei einer angenommenen durchschnittlichen Gültigkeitsdauer von drei Jahren 50.000 ausgestellten Zertifikaten pro Jahr oder circa 1.000 pro Woche. Wenn die Kapazität, um Spitzenzeiten abfedern zu

---

[407] Am Beispiel von RSA bedeutet dies, daß zwar eine große Zahl nicht mittels eines Algorithmus in ihre Faktoren zerlegt werden kann, jedoch nicht ausgeschlossen ist, daß jemand die Faktoren rät und mittels Multiplikation verifiziert.

Vgl. Kapitel 2.2.4 und Kapitel 2.2.6.

[408] Denn der Angreifer verfügt über die Möglichkeit, eigene Zertifikate zu erstellen.

[409] Da diese wiederum mittels dem Zertifikat der RegTP signiert wurden.

können, auf die fünffache Zahl, entsprechend 5.000 Zertifikaten pro Woche, ausgelegt ist, so würden immer noch 30 Wochen vergehen, bis jeder Nutzer sein neues Zertifikat in Händen hielte. Selbst durch großzügige Aufstockung des Personals wird sich dieser Zeitraum aufgrund der nötigen Einarbeitungszeit nicht wesentlich verkürzen lassen. Die Gesamtkosten des Schadensfalls wären die geschilderten Kosten für eine Zertifizierungsstelle multipliziert mit der Anzahl der betroffenen Zertifizierungsstellen[410].

4.4.4 Kompromittierung eines eingesetzten Verfahrens

Da sämtliche eingesetzten Verfahren zur Erstellung digitaler Signaturen mathematischer Art sind, tritt der Fall der Kompromittierung eines eingesetzten Verfahrens ein, sobald eine beliebige Person eine neue Methode entdecken sollte, die eines der zugrundeliegenden Probleme löst[411]. Aufgrund der Anstrengungen, die Mathematiker überall auf der Welt unternehmen, um beispielsweise das Problem der Faktorisierung zu lösen[412], kann davon ausgegangen werden, daß ein neues Verfahren nicht geheim bleiben könnte beziehungsweise, aufgrund des gemeinsamen Fortschritts, nur geringe Zeit später von anderen Mathematikern entdeckt werden würde[413]. Aufgrund der schon seit langer Zeit[414] diskutierten Versuche, dieses Problem zu lösen, kann außerdem davon ausgegangen werden, daß dies hinreichend schwer und die Wahrscheinlichkeit einer zufälligen Lösung gering ist[415].
Der geringen Wahrscheinlichkeit der Kompromittierung eines Verfahrens steht jedoch ein erhebliches Schadenausmaß gegenüber. Neben der Neuausstellung aller

---

[410] Die exakten Kosten werden in Kapitel 5.2.2 ermittelt.

[411] Vgl. Langenbach/Ulrich (Elektronische Signaturen, 2002), S. 24;
Ausführlicher vgl. Langenbach/Ulrich (Elektronische Signaturen, 2002), S. 100ff;
Vgl. Fox (Misserfolgsbegeisterung, 2001), S. 314.

[412] Vgl. Buchmann (Faktorisierung großer Zahlen, 1999), S. 114.

[413] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 119.

[414] Damit ist ein Zeitraum von mehreren hundert Jahren gemeint. Für detailliertere Angaben siehe Buchmann (Wie sicher kann Sicherheit sein, 2001), S. 4ff.

[415] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 119.

Zertifikate ist zu untersuchen, inwiefern die vorhandene Software für andere Algorithmen einsetzbar ist. Ist dies nicht der Fall, muß zusätzlich die Software aller Benutzer und die der Zertifizierungsstelle ausgetauscht beziehungsweise erst erstellt werden. Dies bedeutet, daß zum finanziellen Aufwand noch ein erheblicher logistischer Aufwand hinzukommt[416].

Dies könnte jedoch vermieden werden, in dem von vorne herein Software verwendet wird, die für multiple Verfahren ausgelegt ist. In diesem Fall bliebe der Austausch aller Zertifikate, der sich durch den gleichzeitigen Einsatz mindestens zweier Verfahren erheblich vereinfachen ließe, da zumindest ein mögliches Verfahren bliebe. Dies wäre ausreichend, um beispielsweise den Empfang des neuen Zertifikates bestätigen zu können. Voraussetzung ist demnach eine Software, die grundsätzlich mindestens zwei Verfahren gleichzeitig benutzt oder die Wahl eines Verfahrens dem Benutzer überläßt und Chipkarten, auf denen nicht nur der private Schlüssel eines Verfahrens abgelegt ist oder verschiedene Chipkarten für die unterschiedlichen unterstützten Verfahren[417].

4.4.5 Kompromittierung aller eingesetzten Verfahren

Diese Überlegungen bezüglich des Einsatzes mehrerer Verfahren sind unnötig, wenn die Kompromittierung aller eingesetzter Verfahren zum Beispiel durch den Bau eines Quantencomputers erfolgen würde. Die Wahrscheinlichkeit kann nach dem heutigen Stand der Wissenschaft, die sich zur Zeit mit der Hardware eines solchen Computers beschäftigt, für die nächsten Jahre als gering eingestuft werden[418]. Jedoch könnte eine revolutionäre Methode zur Lösung eines Verfahrens gleichzeitig die Lösung aller Verfahren bedeuten, so daß diese Wahrscheinlichkeit zusätzlich zu berücksichtigen ist[419].

---

[416] Vgl. Kapitel 3.2.2.4.

[417] Der FlexiProvider von FlexiPKI beherrscht beispielsweise mehrere Verfahren. Vgl. Lehrstuhl TI, TUD (FlexiPKI, 2001), Internet-Quelle.

[418] Vgl. Buchmann (Wie sicher kann Sicherheit sein, 2001), S. 9.

[419] Vgl. Selke (Kryptographie, 2000), S. 66.

Da eine Zertifizierung generell nicht mehr möglich wäre, kämen zum Totalverlust der Investitionen noch eventuelle Schadenersatzforderungen, die allerdings für diesen Fall in den allgemeinen Geschäftsbedingungen (AGB) ausgeschlossen sein sollten. Gleichzeitig wird deutlich, weshalb die Forschung nach neuen Algorithmen einen hohen Stellenwert haben muß.

4.4.6 Angriffe gegen die Verfügbarkeit der Dienstleistungen

Angriffe gegen die Infrastruktur sind eine Möglichkeit, die Verfügbarkeit der Zertifizierungsstelle beziehungsweise die Verfügbarkeit der Internet-Dienstleistungen der Zertifizierungsstelle zu verhindern. Diesen Angriffen muß durch infrastrukturelle Maßnahmen, exemplarisch sind der Gebäudeschutz und die Überwachung zu nennen, und Redundanz vorgebeugt werden. Diese Maßnahmen sichern jedoch nur die Funktionalität der Infrastruktur.

Im Internet können allerdings Angriffe durchgeführt werden, die die Verfügbarkeit trotz funktionstüchtiger Infrastruktur verhindern. Als wichtigster Angriff, der außerdem am leichtesten durchzuführen ist, ist der sogenannte Denial of Service-Angriff (DoS)[420], der aufgrund der Belastbarkeit der Server größtenteils verteilt durchgeführt wird. Aus diesem Grund wird von von Distributed Denial of Service-Angriffen (DDoS) gesprochen. Bei diesen Angriffen werden Server mit einer Vielzahl von unnötigen, gefälschten Anfragen konfrontiert, die sie nicht mehr bewältigen können. Da in diesem Fall ebenfalls keine Bearbeitung der regulären Anfragen erfolgt, ist der Server faktisch nicht mehr erreichbar, obwohl die Infrastruktur intakt ist[421].

Für eine Zertifizierungsstelle bedeutet dies im schlimmsten anzunehmenden Fall, daß keine im Internet angebotene Dienstleistung erreichbar ist. Der Zeitraum dieses Zustandes variiert im Bereich mehrerer Stunden[422].

---

[420] Vgl. Schneier (Secrets & Lies, 2001), S. 174.

[421] Vgl. Schneier (Secrets & Lies, 2001), S. 177ff.

[422] Vgl. Rötzer (ECommerce-Websites lahmgelegt, 2000), Internet-Quelle.

4.5 Möglicher Einsatz von Zertifikaten

Mit zunehmender Verbreitung elektronischer Geschäftsvorfälle, nicht nur im Business-to-Business (B2B) sondern auch im Business-to-Customer (B2C), Business-to-Administration (B2A) und Customer-to-Administration (C2A)[423], wird auch der Bedarf an Zertifikaten ansteigen. Im optimistischsten Fall, der vollständigen Verlagerung aller elektronischen Nachrichten auf ein sicheres Niveau, benötigt jeder Bürger der Welt mindestens ein Zertifikat, um am öffentlichen Leben teilnehmen zu können. Allerdings ist dies gegenwärtig kein realistisches Szenario, auch nicht für die nahe Zukunft.

Insofern ist bis auf weiteres davon auszugehen, daß Zertifikate eine Option bleiben, die jeder benutzen kann, aber nicht muß. Dementsprechend müssen aus dem Einsatz von Zertifikate Nutzen oder Zeitersparnisse für die Teilnehmer resultieren, die die damit verbundenen Kosten und Einarbeitungszeiten kompensieren. Der Zeitbedarf der Teilnehmer ist jedoch schwer einzuschätzen ist und von der technischen Qualifikation des Nutzers abhängig. Außerdem differiert der Wert der Zeit der einzelnen Teilnehmer ebenfalls stark. Anders verhält es sich bei den Kosten eines Zertifikates, die ermittelt werden können, indem der potentielle Teilnehmer Angebote der Preise von Zertifikaten bei am Markt existierenden Anbietern einholt.

Auf Angebotsseite ist der Preis eines Zertifikates keinesfalls leicht zu bestimmen, da neben den eigenen Kosten vor allen Dingen die Anzahl der verkauften Zertifikate eingeschätzt werden muß. Die abgesetzte Menge an Zertifikaten hängt jedoch eng mit dem von der Zertifizierungsstelle festgesetzten Preis zusammen, da die Zahl der genutzten Zertifikate mit sinkendem Preis ansteigt. Dies läßt sich durch die Preis-Absatz-Funktion graphisch veranschaulichen[424], die in Abbildung 4-14 zu sehen ist.

---

[423] Vgl. Merz (Electronic Commerce, 1999), S. 20.

[424] Vgl. Feess-Dörr (Microökonomie, 1995), S. 274ff.

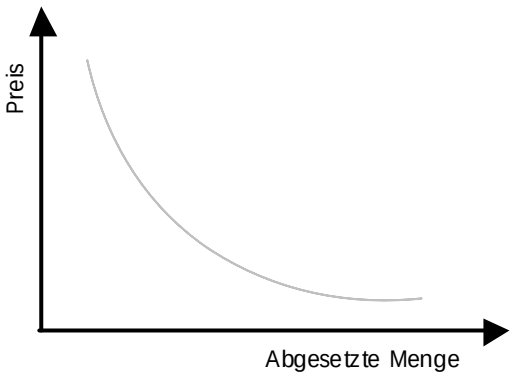

Abbildung 4-14 - Preis-Absatz-Funktion

Quelle: Vgl. Feess-Dörr (Microökonomie, 1995), S. 279.

Zertifikate müssen interoperabel sein[425], das heißt, bei der Nutzung spielt es für den Teilnehmer keine Rolle mehr, welches Zertifikat er verwendet. Der Gesetzgeber dokumentiert dies durch die Signaturinteroperabilitätsspezifikation, die ein Rahmen definiert. Aus dem frühen Marktstadium von Zertifizierungsstellen und der geringen Verbreitung ergibt sich jedoch, daß dies zum heutigen Zeitpunkt noch nicht der Fall ist[426], und daß dieser Prozeß der Standardisierung noch einige Jahre dauern wird[427]. Daß dies unbedingt erfolgen muß steht außer Frage, da ansonsten Hemmschwellen aufgebaut werden können, die den Wechsel des Anbieters erschweren und damit die Möglichkeit für den Anbieter darstellen, höhere Preise am Markt durchzusetzen. Dies wäre für die Verbreitung von Zertifikaten hinderlich und würde die Akzeptanz[428] der Teilnehmer zusätzlich schmälern[429].

Neben den geringen Kosten müssen allerdings Anwendungsfälle geschaffen werden, in denen der Nutzer eines Zertifikates Vorteile hat[430]. Ausgehend von diesen Überlegungen wird in den folgenden Kapiteln der Bedarf an Zertifikaten von ver-

---

[425] Vgl. BSI (SigI, 1999), Internet-Quelle;
Vgl. Esslinger/Barcklow/Bartosch (Global PKI and S/MIME Interoperability, 2001), S. 522.

[426] Vgl. Schwemmer ((Why) It's a long Way to Interoperability, 2001), S. 526.

[427] Vgl. Fox (Cross-Zertifikat, 2001), S. 105.

[428] Eine grundsätzliche Betrachtung der Akzeptanz von Sicherheitsmethoden findet sich in Schultz/Proctor/Lien/Salvendy (Usability and Security, 2001), S. 622.

[429] Vgl. Böhmer (Erfahrungen beim Einsatz und Aufbau einer PKI, 2001), S. 450.

schiedenen Personengruppen ermittelt. Neben der Anzahl an Zertifikaten sollen außerdem die unterschiedlichen notwendigen Sicherheitsniveaus evaluiert werden. Als erstes werden öffentliche Einrichtungen und Unternehmen, das heißt der Bedarf der Angestellten, untersucht. Im Zuge der Privatisierung von Staatsbetrieben, kann die öffentliche Verwaltung als Unternehmen betrachtet werden, zu mal diese aus wirtschaftlichen Gesichtspunkten wie ein solches am Markt auftreten sollte. Daher werden im folgenden die öffentliche Verwaltung und Unternehmen unter dem Begriff Unternehmen zusammengefaßt. Im Anschluß daran wird der Bedarf von Endkunden, den privaten Nutzern, näher betrachtet. Da Kommunikation immer zwei Kommunikationspartner voraussetzt, werden beide Gruppen jeweils aus Sicht des Unternehmens und des Endkunden betrachtet. Die Segmentierung wird in Tabelle 4-1 übersichtlich dargestellt, wobei sich der Bedarf aus Mengen an verkauften Zertifikaten unterschiedlicher Sicherheitsniveaus zusammensetzt. Während innerhalb eines Unternehmens elektronische Kommunikation vorgenommen wird ist dies bei Endkunden nicht der Fall, so daß bereits an dieser Stelle konstatiert werden kann, daß dieses Segmentes über keinen Bedarf verfügt.

		Aus Sicht des	
		Unternehmens	Endkunden
Extern	Unternehmen		
Intern	Endkunden		
	Unternehmen		Keine

Tabelle 4-1 – Klassifikation des Bedarfs an Zertifikaten

4.5.1 Unternehmen

Um den Bedarf an Zertifikaten für die Mitarbeiter von Unternehmen abschätzen zu können, muß die elektronische Kommunikation in zwei Bereiche unterteilt werden. Zum einen in den internen Bereich, der Prozesse betrifft, die innerhalb des Unternehmens von mehreren Personen durchgeführt werden und die aus die-

[430] Vgl. Paulus (Rundum-sorglos Paket mit Hindernissen, 2001), S. 530.

sem Grund miteinander kommunizieren und Dokumente austauschen. Zum anderen in den externen Bereich, der die Kommunikation zwischen Mitarbeitern und Kunden des Unternehmens betrifft. Diese Kunden können Bürger, Unternehmen oder öffentliche Einrichtungen sein.

Extern

Für die elektronische Kommunikation mit Geschäftspartnern sind die Anforderungen Vertraulichkeit und Authentifikation[431] von entscheidender Bedeutung. Dabei tritt nicht die Unterscheidung der Kunden in Endkunden und Unternehmen bei der Wahl des Sicherheitsniveaus zum Vorschein, sondern der Wert der durch die digitale Signatur abgesicherten Transaktion. Deshalb können unterschiedliche Sicherheitsniveaus für verschiedene Prozesse notwendig sein[432]. Selbst für Mitarbeiter und Kunden können diese im gleichen Prozeß differieren[433]. Daher sollte jede Kommunikation verschlüsselt und signiert durchgeführt werden[434]. In manchen Bereichen wäre es nicht notwendig, die Kommunikation vertraulich abzuwickeln. In diesem Fall würden wichtige Daten aufgrund der Verschlüsselung auffallen, weshalb sämtliche Daten verschlüsselt gesendet werden müßten.
Der geschilderte Sachverhalt kann mit folgendem Beispiel veranschaulicht werden. Ein Mitarbeiter eines Unternehmens ist für die Gehaltsverhandlungen zukünftiger Mitarbeiter zuständig und kommuniziert aus diesem Grund elektronisch mit den Bewerbern. Bis auf die konkreten Angebote des Unternehmens verläuft die gesamte Kommunikation zwischen dem Mitarbeiter und den Bewerbern unverschlüsselt über ein unsicheres Netz wie das Internet[435], da dies für den Mitarbeiter komfor-

---

[431] Vgl. Kapitel 2.1.

[432] Während für die Beantragung eines neuen Personalausweises der Kunde ein Zertifikat der höchsten Sicherheitsstufe benötigt, ist dies für die Beantragung einer Meldebestätigung nicht notwendig.

[433] Ein Beispiel ist die Unterscheidung zwischen dem Antrag und der Ausstellung einer Meldebescheinigung einer Stadt.

[434] Vgl. Schneier (Secrets & Lies, 2001), S. 32.

[435] Vgl. Kapitel 2.3.

tabler ist. Auf die zusätzlichen Schritte zur Verschlüsselung und Signatur kann verzichtet werden, weil die konkreten Angebote nur einen sehr geringen Anteil seiner Kommunikation einnehmen. Ein weiterer zukünftiger Bewerber möchte seine Verhandlungsposition verbessern, indem er versucht in die Angebote des Mitarbeiters mittels Abhören Einsicht zu erhalten. Zunächst muß dieser die vollständige Kommunikation des Unternehmens abhören und die Mitteilungen des abzuhörenden Mitarbeiters herausfiltern und nach Gehaltszahlen durchsuchen. Dabei wird er feststellen, daß in den unverschlüsselten Nachrichten die gewünschten Daten nicht enthalten sind. Daraus schließt er, daß diese in den verschlüsselten Nachrichten enthalten sein müssen und beginnt, diese zu entschlüsseln. Wenn es ihm nun gelingen sollte, sei es zufällig, eine Nachricht zu entschlüsseln, so ist er im Besitz der gewünschten Daten. Hätte der Mitarbeiter des Unternehmens jegliche Nachrichten verschlüsselt, so wäre im Falle einer Entschlüsselung einer Nachricht mit hoher Wahrscheinlichkeit eine Nachricht gewählt worden, die keine sensiblen Daten enthält, da diese wesentlich häufiger sind.
Aus diesen Überlegungen ergibt sich, daß ein Großteil der Mitarbeiter mit Zertifikaten niedriger Sicherheitsstufen auskommt, während wenige Personen Zertifikate der höchsten Sicherheitsstufe benötigen.

Intern

Bei der internen Kommunikation sind ebenfalls Zertifikate einzusetzen. Da diese jedoch ausschließlich innerhalb der eigenen Infrastruktur abläuft, genügen Zertifikate eines niedrigen Sicherheitsniveaus. Dies steht in Einklang mit den Anforderungen eines effizienten Informationsflusses innerhalb des Unternehmens, da höhere Sicherheitsstufen mit höheren Anforderungen an die Benutzer korrespondieren.

4.5.2 Endkunden

Endkunden sind alle möglichen Teilnehmer einer Zertifizierungsstelle, die keinem Unternehmen angehören, beziehungsweise ihre Aktionen privat und nicht als Mitarbeiter tätigen.

Um den Bedarf eines Endkunden nach der Art der Zertifikaten abschätzen zu können, müssen die möglichen Kontakte zu Unternehmen und anderen Endkunden untersucht werden.

Unternehmen

Tritt der Endkunde als Kunde in Kontakt mit einem Unternehmen, so richtet sich sein Bedarf an Sicherheit, und damit an die Vertrauenswürdigkeit des Zertifikates, nach dem Wert der Transaktion, die getätigt werden soll. Während beim Kauf von Wirtschaftsgütern zu geringen Kosten dem Unternehmen ein Zertifikat mit einem geringen Sicherheitsniveau ausreichen wird, wird dies mit steigendem Transaktionswert zunehmen. Dies deckt sich mit der Erfahrung, daß bei Bestellungen mit hohem Wert manchmal eine Bestätigung per Fax gefordert wird. Mit der Häufigkeit von Transaktionen mit einem Unternehmen wird die Notwendigkeit eines Zertifikates mit hohem Sicherheitsniveau jedoch abnehmen, da ein gegenseitiges Vertrauensverhältnis entsteht. Dies ist unter anderem darin begründet, daß das Unternehmen Informationen über den Kunden sammelt und daher sein Verhalten einschätzen kann. Zu beachten ist, daß der Einsatz von Zertifikaten aus Sicht der Endkunden nicht nötig ist, da diese durch §§305ff BGB über ausreichende Rechte verfügen[436]. In diesen Paragraphen wurden die vormals in Form von Satellitengesetzen niedergelegten Verbraucherschutzgesetze wie das Verbraucherkreditgesetz (VerbrKrG), das Fernabsatzgesetz (FernAbsG) sowie das Gesetz zum elektronischen Geschäftsverkehr (EGG) gebündelt und nunmehr in das BGB impaktiert. Im Gegensatz dazu ist es für Unternehmen von Vorteil, wenn Endkunden signierte Daten versenden, da in diesem Fall der Nachweis der Transaktion geführt werden kann.

Mit den vorangestellten Überlegungen kann begründet werden, daß es für Endkunden die bei weitem größten Vorteile bringt, auf den Einsatz von Zertifikaten zu verzichten. Aus diesem Grund sind im folgenden zwei Beispiele von Unternehmen dargestellt, in denen der Einsatz von Zertifikaten Nutzen für Endkunden

---

[436] Vgl. Taeger (Rechtssichere Gestaltung, 2002), S. 134.

bringt, der sich im wesentlichen in beschleunigten Prozessen und damit Zeitersparnis niederschlägt.

Als erster Spezialfall wird die öffentliche Verwaltung, als zweiter eine Universität betrachtet. Die Verwaltung nimmt Aufgaben des Staates wahr, bei denen höchste Sicherheit zu gewährleisten ist. Zu den wichtigsten zählen hier die Beantragung und Ausgabe von Ausweisen und die Einreichung der Steuererklärung. Diese Dienste benötigt der Endkunde jedoch selten, erfolgt doch die Steuererklärung in jährlichem Zyklus, die Erneuerung des Personalausweises und Reisepasses in 5 bis 10 jährigem Turnus[437]. Dementsprechend gering ist die Bereitschaft, für ein Zertifikat Kosten aufzuwenden, was sich in den geringen Nutzerzahlen signaturgesetzkonformer Zertifikate niederschlägt[438].

In Universitäten hingegen wird für die gesamte Kommunikationen der Studenten, abgesehen von der Einschreibung, Rückmeldung und Exmatrikulation, nur ein minimales Sicherheitsniveau benötigt. Zwischen beiden Sicherheitsniveaus könnten Prozesse zur Ausstellung von Leistungsnachweisen angesiedelt werden, die zur vollständigen elektronischen Abbildung einen sicheren Nachweis der Identität benötigen. Daß für Klausuranmeldungen oder Kommunikation mit den Fachgebieten ein minimales Sicherheitsniveau ausreichend ist, wird zum einen durch die bereits heute fast vollständig elektronisch ohne den Einsatz von Signaturen abgewickelte Kommunikation deutlich, zum anderen durch die keine hohe Fälschungssicherheit bietenden Studentenausweise. Die Zahl der durchgeführten Transaktionen liegt bei mehreren pro Jahr, so daß sich hier ein bedeutendes Nutzerpotential verbirgt. Zusätzlich bieten sich auf Seiten der Universitätsverwaltung Einsparpotentiale durch die Automatisierung der Prozesse. Allerdings darf der Preis eines Zertifikates keine Hemmschwelle darstellen, da ansonsten weiterhin auf die Nutzung ver-

---

[437] Zwischen dem 16. und 25. Lebensjahr werden die Ausweise um 5 Jahre verlängert, ab dem 26. Lebensjahr um 10 Jahre.

Vgl. Bundesdruckerei GmbH (Personalausweis/Reisepaß, 2001), Internet-Quelle.

[438] Vgl. Hattenberger (Der virtuelle Behördenweg, 2001), S. 541;

Vgl. Fox (Preis der Pioniertat, 2001), S. 62;

Vgl. o.V. (Markt noch nicht reif, 2002), S. 1.

zichtet wird. Letztlich ist, wie bei sämtlichen Transaktionen, das mögliche Schadenausmaß im Falle eines Mißbrauchs als Maßstab der nötigen Sicherheit zu betrachten.

Endkunden

Möchten zwei Endkunden miteinander eine elektronische Transaktion abwickeln, hängt der Sicherheitsbedarf ebenfalls vom Transaktionswert ab. Geht man davon aus, daß der Großteil der Transaktionen nur über einen geringen Wert verfügt, sind Zertifikate mit einem geringen Sicherheitsniveau ausreichend. Darüber hinaus haben sich bei den heutigen Internet-Tauschbörsen, die den bei weitem häufigsten Fall der Endkundentransaktionen stellen, Vertrauensmechanismen etabliert, die die Funktion von Zertifikaten übernehmen und diese damit überflüssig machen. Da sich die Teilnehmer dieser Tauschbörsen ihren Vertrauensstatus aber erst durch viele Transaktionen erarbeiten müssen, könnte dies den Einsatz von Zertifikaten mit niedrigem Sicherheitsniveau fördern[439]. Der tatsächliche Anteil der Endkunden mit elektronischen Transaktionen ist zum heutigen Zeitpunkt allerdings als gering einzustufen[440].

4.5.3 Fazit

Es wird ersichtlich, daß sowohl Bedarf an Zertifikaten mit einem niedrigen als auch mit einem hohen Sicherheitsniveau besteht. Dazwischen sind sämtlich Stufen denkbar, da insbesondere der Transaktionswert unterschiedlich eingeschätzt wird. Eine Einführung vieler verschiedener Zwischenstufen stiftet mehr Verwirrung als Nutzen, weil die gegenseitige Abgrenzung der Stufen schwierig wäre, und ist damit in der Praxis nicht sinnvoll. Mit Berücksichtigung der Tatsache, daß für die niedrige Sicherheitsstufe nicht beweisbar sichere Zertifikate eingesetzt werden

---

[439] Gerade wenn unbekannte Teilnehmer nur für eine Transaktion zusammenkommen, ist es wichtig, daß die eingesetzten Zertifikate interoperabel sind.
Vgl. Fell (Interoperabilität in PKI-Anwendungen, 2001), S. 538.

[440] Vgl. Merz (Electronic Commerce, 1999), S. 20ff.

könnten und für die hohe Sicherheitsstufe signaturgesetzkonforme und damit beweisbar sichere Zertifikate, erscheint die Einführung einer Zwischenstufe fraglich. Die Anzahl beweisbar sicherer Zertifikate an insgesamt benötigten Zertifikaten ist gering[441].

Folgende Abbildung 4-15 veranschaulicht den Zusammenhang zwischen dem Bedarf an Zertifikaten und deren Sicherheitsniveau. Die gestrichelte Linie deutet das Verhältnis zwischen beweisbar sicheren und nicht beweisbar sicheren Zertifikaten an.

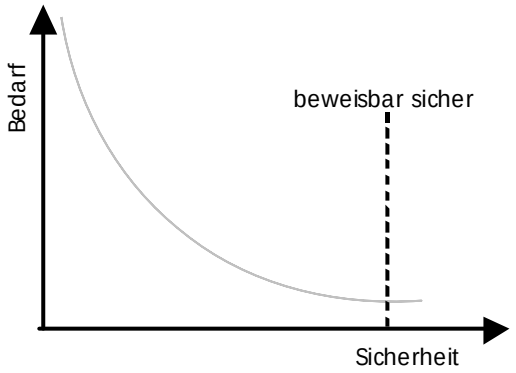

Abbildung 4-15 – Zusammenhang zwischen Bedarf und Sicherheit

[441] Vgl. Fox (Zurück auf dem Boden, 2001), S. 442.

5 Wirtschaftlichkeitsbetrachtung einer Zertifizierungsstelle

Nachdem im vorherigen Kapitel die Rahmenbedingungen für Zertifizierungsstellen dargestellt wurden, wird in diesem Kapitel die Wirtschaftlichkeitsbetrachtung einer Zertifizierungsstelle durchgeführt. Dazu wird im ersten Abschnitt die Vorgehensweise der Wirtschaftlichkeitsbetrachtung erläutert. Die dafür notwendigen Modellannahmen der Zertifizierungsstellen werden im zweiten Abschnitt beschrieben. In den darauffolgenden beiden Abschnitten wird die Kosten- und Erlösbetrachtung durchgeführt, bevor im fünften Abschnitt Fallbeispiele für Zertifizierungsstellen betrachtet werden. Auf diesen Ergebnissen aufbauend erfolgt im sechsten und letzten Abschnitt die Wirtschaftlichkeitsbetrachtung einer Zertifizierungsstelle.

5.1 Vorgehensweise

Um die Wirtschaftlichkeit einer Zertifizierungsstelle messen zu können, müssen Handlungsalternativen nach der Höhe des Erfolgs geordnet und verglichen werden[442]. Dazu werden Wirtschaftlichkeitskennziffern verwendet, die ganz allgemein monetär bewertete Aufwandsgrößen mit monetär bewerteten Ertragsgrößen in Beziehung setzen[443]. Wirtschaftlichkeit wird als Quotient aus Ertrag und Aufwand beziehungsweise Erlöse und Kosten definiert[444]. Ein Wert größer 1 bedeutet, daß die Erlöse die Kosten übersteigen.

---

[442] Vgl. Bohr (Wirtschaftlichkeit, 1993), Sp. 2184.

[443] Vgl. Kuhner (Rentabilität, 2002), Sp. 1696.

[444] Vgl. Bohr (Wirtschaftlichkeit, 1993), Sp. 2186.

Zum Begriff der Wirtschaftlichkeit vgl. auch Bea/Dichtl/Schweitzer (Allgemeine Betriebswirtschaftslehre Bd. 1: Grundfragen, 2000), S. 54f.

Die Wirtschaftlichkeitsbetrachtung einer Zertifizierungsstelle wird über eine Kosten- und Erlösbetrachtung durchgeführt. Als Kalkulationsverfahren kommt die Kosten- und Erlösträgerstückrechnung zum Einsatz[445]. In der Kostenträgerstückrechnung steht die Ermittlung der Kosten im Mittelpunkt, die für die Herstellung und Verwertung einer Mengeneinheit des Kostenträgers entstehen[446]. Die Kostenträgerstückrechnung kann zu einer Erfolgsrechnung ausgebaut werden, indem die je Kostenträgereinheit erzielbaren Erlöse mit einbezogen werden. Dadurch lassen sich Stückerfolge pro Kostenträgereinheit bestimmen, die als Basis für Programmentscheidungen und Erfolgsanalysen herangezogen werden können[447].

Die Kostenträgerstückrechnung kann dabei als Voll-[448] oder Teilkostenrechnung[449] durchgeführt werden[450]. Bei einer Vollkostenkalkulation werden alle, das heißt fixe und variable, Kosten des Unternehmens auf das Produktprogramm verteilt[451]. Dagegen werden in der Teilkostenkalkulation nur Teilkosten[452] bei der Herstellung und Verwertung einer Kostenträgereinheit berücksichtigt[453].

Die Kosten- und Erlösträgerstückrechnung unterscheidet hinsichtlich der Anzahl der Produktarten, der Übereinstimmung der Produkte und der Anzahl der Programmtypen[454]. Im Falle der Produktion einer Produktart mit einem homogenen

---

[445] Vgl. Schweitzer/Küpper (Systeme der Kosten- und Erlösrechnung, 1998), S. 166.

[446] Vgl. Kilger (Flexible Plankostenrechnung, 1993), S. 677.

[447] Vgl. Schweitzer/Küpper (Systeme der Kosten- und Erlösrechnung, 1998), S. 166.

[448] Vgl. Coenenberg (Kostenrechnung und Kostenanalyse, 1999), S. 91.

[449] Vgl. ebenda, S. 114.

[450] Vgl. Mellerowicz (Kosten und Kostenrechnung, 1973), S. 206.

[451] Im Falle einer Zertifizierungsstelle müssen die Kosten nicht verteilt werden, weil eine Einproduktfertigung vorliegt.

[452] Dies können beispielsweise nur Einzelkosten oder nur variable Kosten sein.

[453] Vgl. Schweitzer/Küpper (Systeme der Kosten- und Erlösrechnung, 1998), S. 166.

[454] Vgl. Schweitzer/Küpper (Systeme der Kosten- und Erlösrechnung, 1998), S. 190;
Alternativ könnte zusätzlich Parallelproduktion beziehungsweise unverbundene Produktion, bei der die Produktion des einen Produktes nicht von der eines anderen abhängt, als Kriterium zur Systematisierung benutzt werden. Vgl. Zimmermann (Grundzüge der Kostenrechnung, 1985), S. 109.

Produkt[455], welches in einer Einproduktfertigung hergestellt wird, ist die Divisionsrechnung anzuwenden[456]. Eine Übersicht der Zuordnung der Kalkulationsverfahren zu Typen des Produktionsprogramms bietet Abbildung 5-1. Die Divisionsrechnung stellt das einfachste Kalkulationsverfahren dar[457]. In diesem Verfahren werden die Kosten je Kostenträgereinheit bestimmt, indem die insgesamt in einer Periode angefallenen Kosten durch die Zahl der erstellten Leistungseinheiten des Kostenträgers dividiert werden[458]. Es wird vorausgesetzt, daß die Produktionsmenge identisch mit der Absatzmenge ist[459].

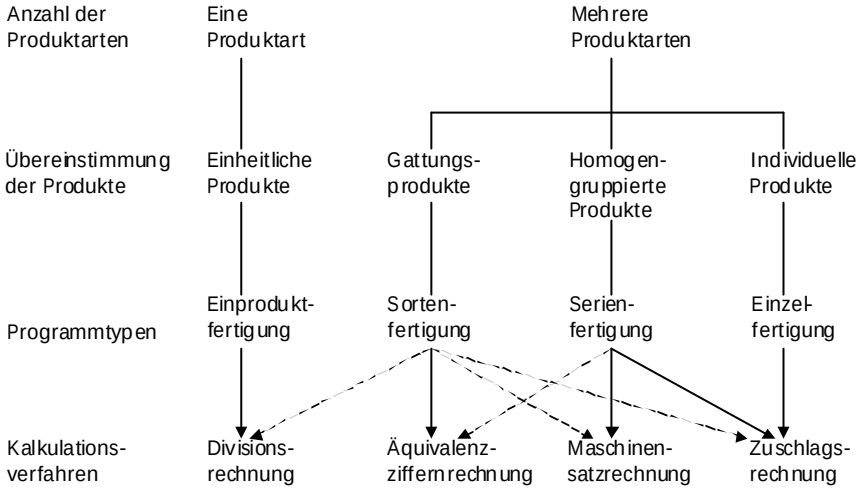

Abbildung 5-1 – Zuordnung der Kalkulationsverfahren zu Typen des Produktionsprogramms

Quelle: Schweitzer/Küpper (Systeme der Kosten- und Erlösrechnung, 1998), S. 190.

---

[455] Eine Zertifizierungsstelle stellt nur das Produkt Zertifikate her. Der Zeitstempel, der als zweites Produkt angesehen werden könnte, wird zusammen mit diesem Produkt verkauft und gehört daher zum Produkt Zertifikat. Die ausführliche Begründung befindet sich in Kapitel 4.3. Damit gehört eine Zertifizierungsstelle zu den Betrieben, bei denen eine Einproduktfertigung vorliegt.

Vgl. Mellerowicz (Kosten und Kostenrechnung, 1973), S. 140.

[456] Vgl. Schweitzer/Küpper (Systeme der Kosten- und Erlösrechnung, 1998), S. 190.

[457] Vgl. Schweitzer/Küpper (Systeme der Kosten- und Erlösrechnung, 1998), S. 167.

[458] Vgl. Bea/Dichtl/Schweitzer (Allgemeine Betriebswirtschaftslehre Bd. 2: Führung, 2001), S. 697.

[459] Vgl. Zimmermann (Grundzüge der Kostenrechnung, 1985), S. 110.

5.2 Modellannahmen

Bevor die Kosten und Erlöse einer Zertifizierungsstelle untersucht werden können, müssen Modellannahmen über die Ausgestaltung derselben getroffen werden. Eine Zertifizierungsstelle setzt sich dabei aus verschiedenen Teilaspekten zusammen. Eine Übersicht der unterschiedlichen Teilaspekte einer Zertifizierungsstelle sowie der zu realisierenden Sicherheitsstufen bietet Abbildung 5-2, bei der die verschiedenen Teilaspekte einer Zertifizierungsstelle auf der horizontalen Achse und die möglichen Sicherheitsstufen auf der vertikalen Achse aufgetragen sind.

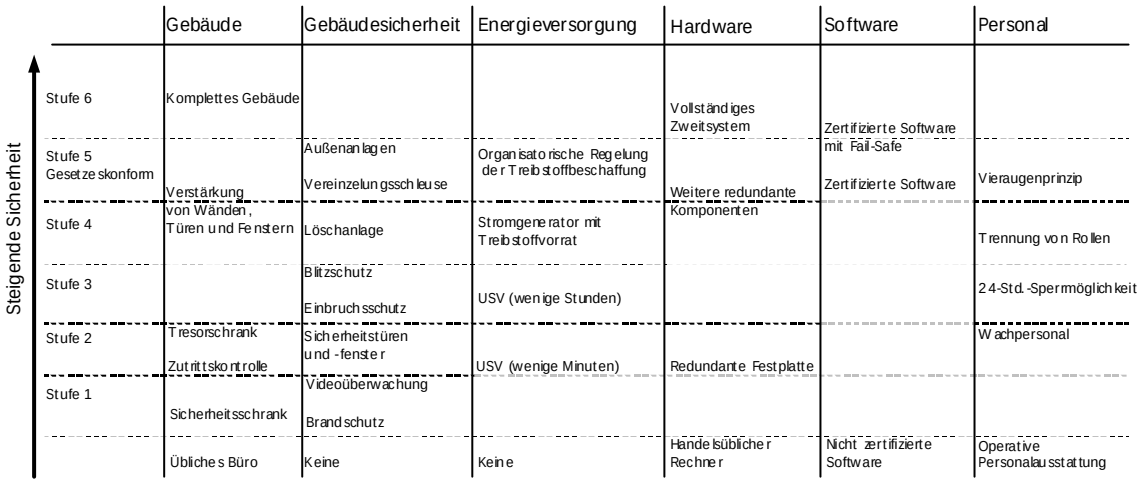

Abbildung 5-2 – Mögliche Sicherheitsstufen der unterschiedlichen Teilaspekte einer Zertifizierungsstelle

Aus Abbildung 5-2 wird deutlich, daß es eine Vielzahl unterschiedlicher Modelle gibt, die sich hinsichtlich der Kosten und des erreichten Sicherheitsniveaus unterscheiden. Die angedeuteten Stufen realisieren in jedem Teilaspekt ein gleich hohes Sicherheitsniveau, wobei das niedrigste Sicherheitsniveau eines Teilaspektes das Sicherheitsniveau der gesamten Zertifizierungsstelle bestimmt. Da nicht sämtliche möglichen Modelle betrachtet werden können, werden in dieser Arbeit zwei Modelle herausgegriffen und näher untersucht, die sich hinsichtlich des erreichten Sicherheitsniveaus gravierend unterscheiden. Zum einen ist dies das Modell einer minimalen Sicherheitsstufe, die durch Stufe 1 der Abbildung realisiert wird. In dieser Stufe wird versucht, die Dienste einer Zertifizierungsstelle anzubieten und

gleichzeitig die Kosten möglichst niedrig zu halten. Zum anderen wird das Modell einer maximalen Sicherheitsstufe beschrieben, realisiert durch Stufe 5 der Abbildung. Die Bezeichnung maximal wird gewählt, da diese Sicherheitsstufe den Anforderungen des Gesetzes hinsichtlich der Ausgabe beweisbar sicherer Zertifikate genügt. Eine Steigerung der Sicherheit über dieses Niveau hinaus ist möglich, aber aus wirtschaftlicher Sicht nicht sinnvoll. Aus juristischer Sicht ist zu bedenken, ob selbst dieses Niveau ausreichend ist.

Das Modell einer minimalen Sicherheitsstufe besteht aus einem tragbaren Rechner, der von zwei Mitarbeitern verwendet wird, um die Dienstleistungen der Zertifizierungsstelle zu erbringen. Die Mitarbeiter benötigen einen Büroraum. Der Rechner verfügt über die notwendige Hardware, um Chipkarten lesen und beschreiben zu können. Wird der tragbare Rechner nicht benötigt, so muß er in einen Sicherheitsschrank weggeschlossen werden, in dem zusätzlich die Dokumente der Zertifizierungsstelle archiviert werden. Außerdem ist er durch einen eigenen Akku von Stromausfällen bis zu 2 Stunden nicht betroffen. Darüber hinaus existiert ein Rechner, der in einem Rechenzentrum untergebracht und jederzeit verfügbar ist. Im Rechenzentrum ist der Rechner physisch geschützt und durch Notstromaggregate von einem Stromausfall nicht betroffen. Das Personal besteht aus einem Verantwortlichen, dessen Tätigkeiten die Ausstellung und Sperrung von Zertifikaten sowie allgemeine Verwaltungstätigkeiten umfassen, und einem Vertreter, der neben Vertretung im Krankheits- und Urlaubsfall für die Wartung der beiden Rechner zuständig ist und ebenfalls allgemeine Verwaltungstätigkeiten übernimmt.

Im Gegensatz dazu wird das Modell einer maximalen Sicherheitsstufe durch ein Gebäude realisiert, das ausschließlich für die Zertifizierungsstelle genutzt wird. Dem Sicherheitsniveau wird durch Verstärkung der Türen, Wände und Fenster ebenso Rechnung getragen wie durch Zutrittskontrollen und Vereinzelungsschleusen. Das gesamte Gebäude muß über den dem Stand der Technik bestmöglich entsprechenden Blitz-, Feuer- und Wasserschutz verfügen. Die Rechner der Zertifizierungsstelle müssen im Fehlerfall weiterlaufen, so daß hier erhöhte Anforderungen an die Hardware bestehen. Zusätzlich wird bei sicherheitsrelevanten Tä-

tigkeiten das Vieraugenprinzip vorgeschrieben. Insgesamt betrachtet führt dies zu einem erhöhten Personalaufwand, sowohl hinsichtlich der Wartung und Pflege der Rechner als auch des normalen Betriebes der Zertifizierungsstelle. Darüber hinaus entsteht durch die umfangreichere Dokumentation ein beträchtlicher Verwaltungsaufwand. Damit die Sperrung von Zertifikaten jederzeit vorgenommen werden kann, muß ebenfalls entsprechend Personal eingesetzt werden. Der Personalaufwand wird später in Abschnitt 5.3.1.3 ermittelt.

Während in diesem Kapitel untersucht wird, ob der wirtschaftliche Betrieb einer Zertifizierungsstelle dieser beiden Sicherheitsniveaus möglich ist, wird in Kapitel 6 das hinsichtlich des Kosten-Sicherheits-Verhältnisses optimale Modell gesucht. Aus diesem Grund wird das Modell des minimalen Sicherheitsniveaus gewählt. Durch schrittweise Erhöhung des Sicherheitsniveaus in einem oder mehreren Teilaspekten können weitere mögliche Modelle gebildet und beurteilt werden, für die jedoch höhere Kosten anfallen. Ist ein wirtschaftliches Betreiben nach dem Modell der minimalen Sicherheitsstufe nicht möglich, kann kein anderes Modell wirtschaftlich betrieben werden. Wenn ein wirtschaftlicher Betrieb möglich ist, ist zu prüfen, ob das Sicherheitsniveau noch erhöht werden kann.

5.3 Kostenbetrachtung einer Zertifizierungsstelle

In diesem Abschnitt werden die Kosten einer Zertifizierungsstelle betrachtet, mit dem Ziel der Bestimmung der Kosten eines ausgestellten Zertifikates. Als Vorgabe wird hier noch keine Wahl bezüglich der im vorherigen Kapitel vorgestellten Rahmenbedingungen für Zertifizierungsstellen getroffen, sondern es werden die zu betrachtenden Kostenarten systematisiert und näher erläutert.

Zur Ermittlung der Kosten für die Erstellung eines Zertifikates werden zuerst die Fixkosten einer Zertifizierungsstelle betrachtet, die sich aus den Infrastrukturkomponenten ergeben. Dazu werden die Kosten der einzelnen Teilaspekte einer Zertifizierungsstelle nacheinander untersucht, jeweils für das Modell einer minimalen Sicherheitsstufe und einer maximalen Sicherheitsstufe. Im zweiten Abschnitt werden die variablen Kosten einer Zertifizierungsstelle ermittelt. Hier wird bereits

berücksichtigt, welche Kosten durch eine geeignete Verteilung der Aufgaben auf die Mitarbeiter der Zertifizierungsstelle eingespart werden können[460]. Im dritten Teil der Kostenbetrachtung werden im darauffolgenden Abschnitt die Risikokosten, die aus den möglichen Angriffen gegen eine Zertifizierungsstelle resultieren können, beschrieben. Dazu werden mögliche Risiken für die Zertifizierungsstelle aufgeführt, die im Einzelfall unter Berücksichtigung der realisierten Zertifizierungsstelle ermittelt werden müssen. Diese müssen bei der Umlage der Kosten auf ein Zertifikat als Bestandteil der Kosten eines Zertifikates einbezogen werden, womit sich der letzte Abschnitt beschäftigt. Das Geschäftsmodell einer Zertifizierungsstelle muß gewährleisten, daß ein Schadensfall nicht den Fortbestand gefährdet oder beendet[461].

Die beschriebene Vorgehensweise dieses Abschnitts wird durch das in Abbildung 5-3 dargestellte Schema der für eine Zertifizierungsstelle relevanten Kostenarten verdeutlicht. Aus der Abbildung geht hervor, daß die Risikokosten weder allein den fixen noch ausschließlich den variablen Kosten zuzuordnen sind. Vielmehr muß detailliert jedes mögliche Schadenpotential auf die Zuordnung zu fixen oder variablen Kosten untersucht werden. Wegen der nicht eindeutigen Zuordnung werden in der vorliegenden Arbeit die Risikokosten als dritter Block nach den fixen und variablen Kosten betrachtet. Die Einbeziehung der aufsummierten fixen und variablen Risikokosten in die fixen und variablen Kosten ermöglicht die Ermittlung der Gesamtkosten eines Zertifikates unter Berücksichtigung der zugrundeliegenden Zahl verkaufter Zertifikate.

---

[460] Beispielsweise könnte der Wachdienst zusätzlich Aufgaben des Sperrdienstes übernehmen.

[461] Vgl. Blum (Entwurf eines neuen Signaturgesetzes, 2001), S. 74.

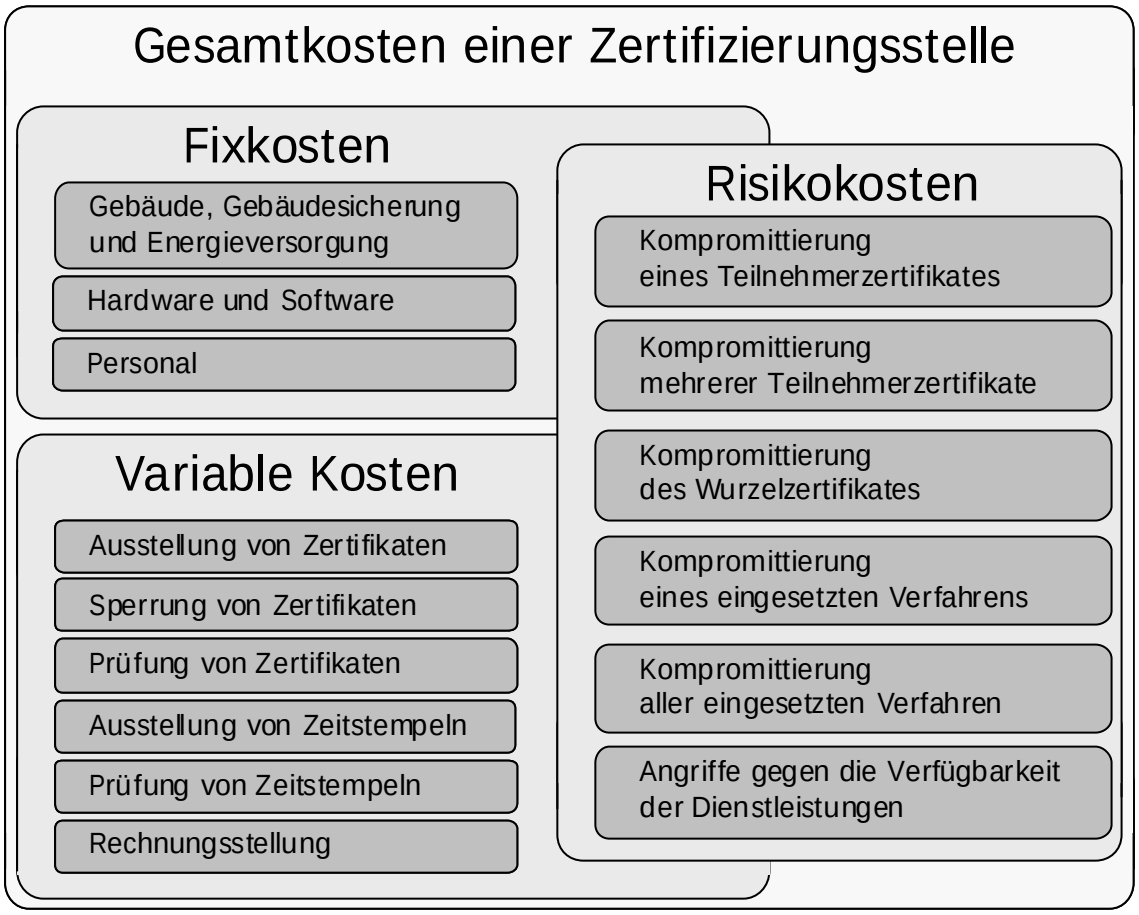

Abbildung 5-3 – Allgemeines Schema der für Zertifizierungsstellen relevanten Kostenarten

5.3.1 Fixkosten einer Zertifizierungsstelle

Bei der Betrachtung der Fixkosten einer Zertifizierungsstelle wird im ersten Abschnitt mit den Kosten des Gebäudes, der Gebäudesicherung und der Energieversorgung begonnen. Da sich diese gegenseitig beeinflussen, ist eine gemeinsame Betrachtung sinnvoll. An dieser Stelle werden einzelne Schadensfälle, beispielsweise der Ausfall der Stromversorgung, bereits berücksichtigt. Im zweiten Abschnitt werden die notwendigen Kosten für Hard- und Software ermittelt, während im letzten Abschnitt die Kosten für die Mitarbeiter der Zertifizierungsstelle betrachtet werden.

5.3.1.1 Gebäude, Gebäudesicherung und Energieversorgung

Die Kosten des Gebäudes richten sich nach dem Standort und der Gebäudegröße, insbesondere aber nach dem Sicherheitsniveau der Zertifizierungsstelle. Während im Falle einer signaturgesetzkonformen Zertifizierungsstelle die gesetzlichen Anforderungen[462] einzuhalten sind, ist das Gebäude im anderen Fall nach eigenem Ermessen zu planen.

Um die deutlichen Kostenunterschiede dennoch einordnen zu können und eine sinnvolle Wahl der zu bauenden Zertifizierungsstelle zu treffen, sind zwei wesentliche Punkte zu beachten. Zum einen ist die Gesamtsicherheit eines Gebäudes immer nur so stark wie der schwächste Teil[463], zum anderen kann die Sicherheit sukzessive durch einzelne Maßnahmen[464] erhöht werden.

Das Modell der minimalen Sicherheitsstufe wird durch einen tragbaren Rechner realisiert, der in dem Büro eines Mitarbeiters untergebracht wird. Dieser verfügt über die notwendige Software, um die Dienstleistungen einer Zertifizierungsstelle zu erbringen und ermöglicht die Ausstellung personalisierter Zertifikate mittels eines Chipkartenschreibgerätes.

Ausgehend von diesem Modell kann die Sicherheit der Zertifizierungsstelle schrittweise erhöht werden, so daß nur die Entscheidung zu treffen ist, welche Investitionshöhe welchen Grad zusätzlicher Sicherheit rechtfertigt. Eine Übersicht möglicher Stufen, die zur Erhöhung des Sicherheitsniveaus des Gebäudes genutzt werden können, gibt Abbildung 5-4.

---

[462] Diese ergeben sich aus dem Sicherheitskonzept nach §4 Abs. 2 (4) des SigG, dessen Inhalt in der SigV in §2 spezifiziert wird. Dieses sieht unter 1. eine Beschreibung aller technischen, baulichen und organisatorischen Sicherheitsmaßnahmen und deren Eignung vor. Unter Berücksichtigung des BSI (IT-Grundschutzhandbuch, 2001) ergeben sich die in Kapitel 3.2.2.1 geschilderten Anforderungen.

[463] Vgl. Schneier (Secrets & Lies, 2001), S. 263.

[464] Vgl. BSI (IT-Grundschutzhandbuch, 2001), Kapitel 4.1.

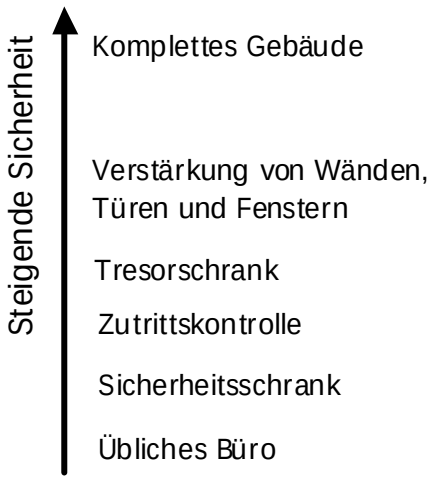

Abbildung 5-4 – Stufenweise Erhöhung des Sicherheitsniveaus des Gebäudes

Im Modell einer maximalen Sicherheitsstufe werden sämtliche in der Abbildung 5-4 genannten Stufen realisiert. Es ist ein Gebäude vorgesehen, das ausschließlich für die Zertifizierungsstelle genutzt wird. Dies bietet zugleich die bestmögliche Form der wirtschaftlichen Gestaltung von Sicherungsmaßnahmen. Die nächste zu treffende Entscheidung ist der Standort, der die Kosten wesentlich beeinflußt. Zu berücksichtigen ist jedoch, daß bei einem Gebäude in einer größeren Stadt den höheren Kosten eine leichtere Erreichbarkeit durch die potentiellen Teilnehmer gegenübersteht. Weitere Kriterien der Standortwahl sind Erschütterungen naher Verkehrswege, Hochwassergefährdung oder die Nähe von Sendeeinrichtungen[465]. Nach der Wahl des Standortes muß die Entscheidung bezüglich der Gestaltung des Gebäudes getroffen werden. Dabei ist es empfehlenswert, schutzbedürftige Räume im Zentrum des Gebäudes zu plazieren[466].

Möglich ist die Nutzung nur eines Stockwerkes, auf das sämtliche Räume verteilt werden. Um beispielsweise sicher vor einer Überflutung des Serverraumes zu sein, bietet jedoch sich ein Gebäude an, dessen Räume auf mehrere Stockwerke verteilt sind. In diesem Fall kann die Technik im Keller- und Obergeschoß redundant untergebracht werden, wodurch ein besserer Schutz vor dem Ausfall beider Systeme

[465] Für nähere Informationen zur geeigneten Standortauswahl vgl. BSI (IT-Grundschutzhandbuch, 2001), M 1.16.

[466] Vgl. BSI (IT-Grundschutzhandbuch, 2001), M 1.13.

gewährleistet ist[467]. Bei der Verteilung der Räume sind damit ebenfalls viele Variationen möglich, die das Sicherheitsniveau beeinflussen, beziehungsweise von unterschiedlicher Kostenintensität sind.

Die Gebäudesicherung hat im wesentlichen zwei Aufgaben zu bewältigen. Unberechtigter Zugang zur Zertifizierungsstelle muß zum einen unterbunden und zum anderen, im günstigsten Fall bereits der Versuch desselben, erkannt werden. Dies muß durch bauliche Maßnahmen, technische Vorkehrungen und Wachpersonal gewährleistet werden. Die Ausgestaltung der Maßnahmen wird durch die zu erreichende Sicherheitsstufe bestimmt.

Im Modell der minimalen Sicherheitsstufe ist die Zertifizierungsstelle vor unberechtigtem Zugriff durch die Unterbringung des Rechners der Zertifizierungsstelle in einem Sicherheitsschrank geschützt. Der Sicherheitsschrank muß darüber hinaus über ausreichenden Brandschutz verfügen. Ob in dieser Sicherheitsstufe eine Videoüberwachung des Sicherheitsschrankes nötig ist, muß im Einzelfall unter Berücksichtigung der Gebäudesicherung des Gesamtkomplexes beurteilt werden.

Die genannten Sicherheitsmaßnahmen sind für das Modell der maximalen Sicherheitsstufe bei weitem nicht ausreichend. Abbildung 5-5 bietet eine Übersicht weiterer Sicherheitsmaßnahmen zur Erhöhung des Sicherheitsniveaus der Gebäudesicherung, die zusätzlich eingesetzt werden können.

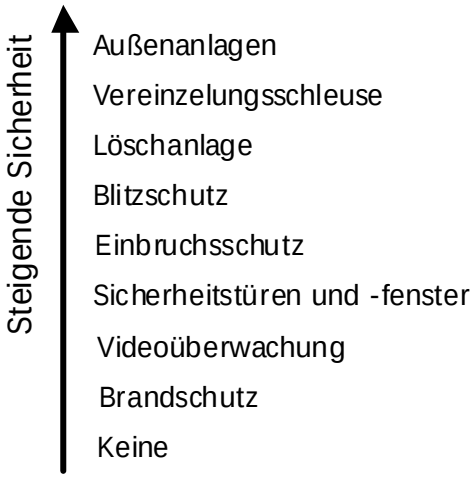

Abbildung 5-5 - Stufenweise Erhöhung des Sicherheitsniveaus der Gebäudesicherheit

[467] Vgl. BSI (IT-Grundschutzhandbuch, 2001), M 1.13.

In den Modellannahmen wurde spezifiziert, daß für das Modell einer maximalen Sicherheitsstufe von einem nur für die Zertifizierungsstelle genutzten Gebäude ausgegangen wird. Dafür sind als wichtigste Maßnahmen der Gebäudesicherung stärkeres Mauerwerk, besondere Türen und Kabelkanäle sowie Vorrichtungen zum Brandschutz und zur Raumüberwachung zu nennen. Um den Schutz des Gebäudes garantieren zu können, muß darüber hinaus ein Sicherheitskonzept erstellt, langfristig durchgeführt und überwacht werden[468]. Dieses Sicherheitskonzept muß gewährleisten, daß die in Kapitel 3.2.2 beschriebenen Sicherheitsmaßnahmen erfüllt sind, die durch die gesetzlichen Regelungen gefordert werden. Dazu kommt der Zugangsschutz des Gebäudes von außen, der beliebig erhöht werden kann. Exemplarisch sei der Schutz gegen Terrorismus genannt, der sehr hohe Kosten verursachen kann[469]. Der größere Abstand zu anderen Gebäuden erhöht außerdem den Schutz gegen unerwünschtes Abhören von Daten und das Eindringen aus anderen Gebäuden per Tunnel.

Bezüglich der Energieversorgung ist beim Modell der minimalen Sicherheitsstufe zwischen den beiden Rechnern zu unterscheiden. Während der tragbare Rechner durch den Akku ausreichend geschützt ist, ist dies beim Rechner des Verzeichnisdienstes nicht der Fall, weil dieser permanent verfügbar sein muß. Dies ist durch die Unterbringung in einem Rechenzentrum mit Notstromversorgung gewährleistet.

Im Falle einer Notstromversorgung muß zwischen verschiedenen Stufen unterschieden werden. Wie bereits geschildert, ist die Möglichkeit, auf Notstrom zu verzichten, selbst in der minimalen Sicherheitsstufe nicht ausreichend. Eine höhere Stufe garantiert dies, in dem zumindest so lange Strom vorhanden sein muß, bis die Geräte sicher ohne Datenverlust ausgeschaltet werden können. Eine weitere Stufe wird durch eine mehrstündige Stromversorgung dargestellt, die zumindest

---

[468] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 280;
Nach SigG §4 (3) Satz 3 und SigV §12 (1).

[469] Soll beispielsweise ein Angriff durch Flugzeuge verhindert werden, so ergeben sich daraus deutlich erhöhte Anforderungen an das Gebäude der Zertifizierungsstelle.

eine kurzfristige Aufrechterhaltung des Betriebes ermöglicht. Gesteigert werden kann dies nur noch durch Notstromversorgung mittels Stromgenerator samt Treibstoffvorrat, der in Kombination mit einer organisatorischen Regelung der Treibstoffversorgung für unbegrenzte Zeit die Zertifizierungsstelle mit Strom versorgen könnte. Die ist für das Betreiben einer Zertifizierungsstelle des maximalen Sicherheitsniveaus erforderlich. Den geschilderten Sachverhalt veranschaulicht Abbildung 5-6.

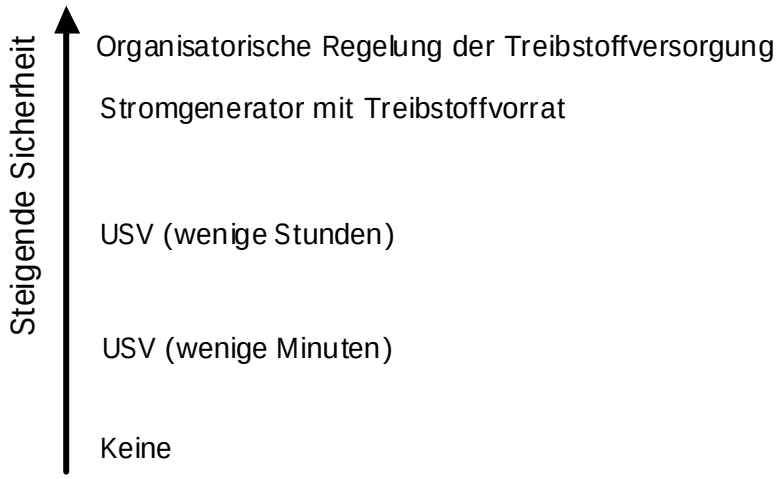

Abbildung 5-6 - Stufenweise Erhöhung des Sicherheitsniveaus der Energieversorgung

5.3.1.2 Hardware und Software

Die Hardware der Zertifizierungsstelle besteht aus Rechnern, die für die Zertifikatserstellung und –verwaltung zuständig sind. Die dazu erforderliche Rechenleistung wird von einem handelsüblichen Rechner bereitgestellt. Redundante Komponenten zur Vermeidung von Ausfällen und der Erhöhung der Verfügbarkeit führen zu höheren Kosten bei der Anschaffung[470]. In der maximalen Sicherheitsstufe ist eine Trennung der Funktionalitäten Dokumentation, Verzeichnis- und Zeitstempeldienst auf mehrere Rechner notwendig. Zu den Rechnern müssen Monitore, Drucker, Chipkarten-Lese- und –Schreibgeräte sowie ein Chipkartendruk-

[470] Vgl. in anderem Zusammenhang Diedrich (Preiswerte Hochleistungsrechner mit Clustern, 2000), S. 234.

ker zur Personalisierung erworben werden. Erst bei einer sehr hohen Zahl an verwalteten Zertifikaten muß dem durch leistungsstärkere Hardware Rechnung getragen werden. Eine Übersicht möglicher Sicherheitsniveaus der Hardware gibt Abbildung 5-7.

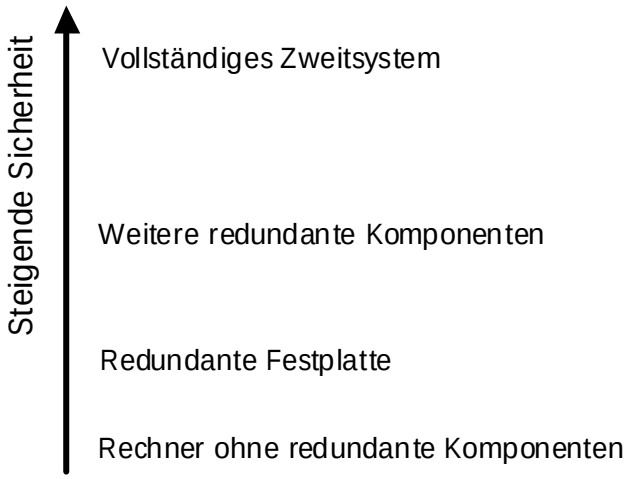

Abbildung 5-7 - Stufenweise Erhöhung des Sicherheitsniveaus der Hardware

Neben der Verfügbarkeit spielt die Abstrahlung der Rechner und der Verkabelung eine wichtige Rolle, da es Angreifern gelingen könnte, durch Abhören von Daten in den Besitz geheimer Schlüssel zu gelangen. Als Verkabelungsart werden daher Glasfaser-Lichtwellenleiter (LWL) genutzt[471]. Weil die Strahlung der Hardware außerhalb der Zertifizierungsstelle nicht abzuhören sein darf, muß diese im Zusammenspiel mit dem schützenden Gebäude betrachtet werden.

Von entscheidender Bedeutung für den Erfolg einer Zertifizierungsstelle ist die verwendete Software. So lange noch keine Standardisierung vorliegt[472] und kryp-

---

[471] Vgl. BSI (IT-Grundschutzhandbuch, 2001), M 5.3.

[472] Auch wenn Zertifikate interoperabel sein sollen und die Spezifikation dafür vorliegt, siehe BSI (SigI, 1999), ist der Zeitpunkt der Realisierung der Interoperabilität nicht abzuschätzen.
Die Sicht einer signaturgesetzkonformen Zertifizierungsstelle, der DATEV, gibt Leistenschneider (Aufbau einer SigG-konformen Zertifizierungsstelle, 2001), S. 47 wieder.
Das Release der Spezifikation der T7-ISIS Organisation erfolgte am 30. November 2001, ein Test soll im Jahr 2002 erfolgen. Siehe T7-ISIS Organisation (ISIS-MTT 1.01 Release, 2001), Internet-Quelle.

tographische Funktionen noch mittels Plug-Ins[473] der Zertifizierungsstelle in bestehende Software eingebunden werden müssen, entscheidet deren Benutzerfreundlichkeit über die Nutzung durch die Teilnehmer[474]. Die höheren Kosten, die durch die aufwendigere Entwicklung entstehen, werden durch die geringeren Kosten der notwendigen Hilfestellungen für Teilnehmer[475] kompensiert.

Mit steigender Zahl an Zertifikaten wachsen die Anforderungen an die Software, da sich die Parallelität des Zugriffs erhöht[476]. Zum einen geschieht dies durch eine größere Anzahl an Mitarbeitern der Zertifizierungsstelle, die Zertifikate ausstellen oder Sperrungen durchführen, zum anderen durch die größere Anzahl von Nutzern, die Zertifikate überprüfen.

Aufgrund der nicht beweisbaren Sicherheit der verwendeten Algorithmen kann es zum Fall der Kompromittierung kommen. In diesem Fall ist entscheidend, ob die verwendete Software modular aufgebaut ist und ob sich die eingesetzten Algorithmen austauschen lassen, ohne die Sicherheit des Systems zu gefährden. Besonders der Austausch der Software auf der Teilnehmerseite ist mit Kosten verbunden, die mit der Anzahl der Teilnehmer steigen. Dies stellt ein Risiko für die Zertifizierungsstelle dar. Insbesondere ist zu beachten, daß die Kosten eines Schadensfalls die Mehrkosten bei der Anschaffung der Software bei weitem übersteigen und daher der Einsatz einer Software mit mehreren verwendbaren Algorithmen zu

---

Ab 2003 soll ISIS-MTT Grundlage für neugeschaffene PKI-Anwendungen sein.

Vgl. Fell (Interoperabilität in PKI-Anwendungen, 2001), S. 538.

[473] Ein Hardware- oder Softwaremodul, welches bestimmte Fähigkeiten oder Services zu einem größeren System hinzufügt.

Vgl. o.V. (Webopedia, 2001), Internet-Quelle.

[474] Vgl. Fritsch (Infrastructure for electronic signature applications, 2001), S. 535;
Vgl. Bonder ("PKIs sind noch nicht alltagstauglich", 2001), S. 24.

[475] Üblicherweise durch Telefonsupport oder Internetseiten angebotene Möglichkeiten für Teilnehmer der Zertifizierungsstelle.

[476] Zum Beispiel ist ein gleichzeitig schreibender und lesender Zugriff mehrerer Benutzer auf die gleichen Daten nicht möglich, so daß Mechanismen geschaffen werden müssen, die diese Zugriffe hintereinander abwickeln, ohne daß es zu Störungen kommt.

empfehlen ist. Mögliche Sicherheitsniveaus, die durch stufenweise Erhöhung erreicht werden können, sind in Abbildung 5-8 dargestellt.

Des weiteren sind Software-Kosten zu berücksichtigen, die für nicht für die Zertifizierungsstelle benötigte Software anfallen, exemplarisch seien Betriebssystemsoftware, Verwaltungssoftware und die Firewall genannt. Diese können jedoch den Kosten der Hardware zugerechnet werden. Neben der Sicherheit ist die Bedienerfreundlichkeit der eingesetzten Software der Zertifizierungsstelle ebenso ein Kriterium wie bei der Software der Teilnehmer, da Bedienungsfehler mit Kosten verbunden sind und aus diesem Grund vermieden werden müssen.

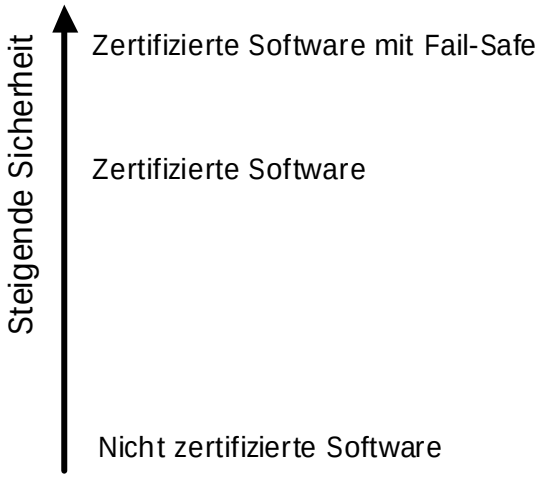

Abbildung 5-8 - Stufenweise Erhöhung des Sicherheitsniveaus der Software

5.3.1.3 Personal

Die Kosten des Personals werden durch das zu erreichende Sicherheitsniveau der Zertifizierungsstelle bestimmt, das festlegt, auf welche Art und Weise die Dienste der Zertifizierungsstelle geleistet werden.

Als erstes ist für den Betrieb der Zertifizierungsstelle ein Verantwortlicher notwendig. Für die Ausstellung und Sperrung von Zertifikaten sowie für die Aufrechterhaltung des technischen Betriebes sind Mitarbeiter nötig. Die Anzahl wird neben dem Sicherheitsniveau durch die geplante Teilnehmerzahl der Zertifizie-

rungsstelle[477] bestimmt. Dies betrifft sämtliche Services innerhalb der Zertifizierungsstelle sowie die für die Überprüfung von Zertifikaten oder Zeitstempeln angebotenen Dienste, die jederzeit von außen erreichbar sein müssen. Hinzu kommen Aufgaben wie die Wartung oder der Austausch von Hardware, das Einspielen von Patches[478] oder Updates oder die Kontrolle der Firewall. An diesem Punkt wird deutlich, daß kostengünstige Lösungen bei der Anschaffung der Software durch höhere Wartungskosten kompensiert werden können. Zuletzt muß genügend Wachpersonal eingeplant werden, um die Zertifizierungsstelle jederzeit überwachen zu können.

Ein höheres Sicherheitsniveau einer Zertifizierungsstelle äußert sich beim Personal nur indirekt. Das Sicherheitsniveau eines Mitarbeiters kann nicht durch einen anderen Mitarbeiter gesteigert werden, sondern nur durch Kontrolle, Vorgaben der Arbeitsdurchführung oder Organisationsanweisungen. Als wichtigster Punkt sei hier das Vieraugenprinzip[479] genannt, das einen erhöhten Personaleinsatz und damit einhergehend höhere Kosten zur Folge hat[480]. Abbildung 5-9 stellt mögliche Sicherheitsstufen der Erhöhung des Sicherheitsniveaus des Personals dar.

---

[477] Die Anzahl der Teilnehmer beziehungsweise der ausgegebenen Zertifikate bestimmt den Zeitaufwand für die Mitarbeiter und damit deren Anzahl.

[478] Ein temporäre Ausbesserung eines Programmfehlers.
Vgl. o.V. (Webopedia, 2001), Internet-Quelle.

[479] Vgl. ARD-Ratgeber Recht (Vieraugenprinzip, 2001), Internet-Quelle.

[480] In Camphausen/Kelm/Liedke/Weber (Aufbau und Betrieb einer Zertifizierungsinstanz, 2001), S. 42 wird der Einsatz des Vieraugenprinzips schon auf mittlerem Sicherheitsniveau zum Beispiel beim Zugriff auf den Signierschlüssel empfohlen.

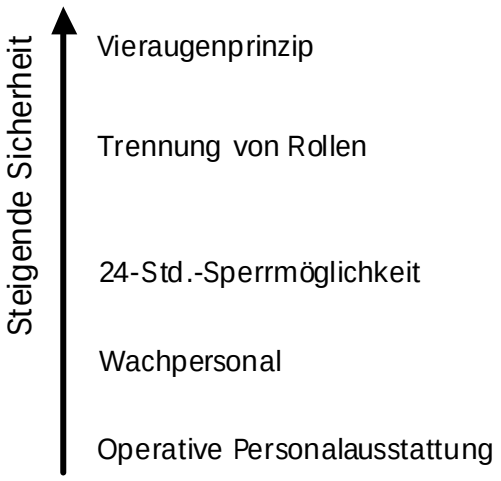

Abbildung 5-9 - Stufenweise Erhöhung des Sicherheitsniveaus des Personals

Eine Zertifizierungsstelle des maximalen Sicherheitsniveaus benötigt einen Verantwortlichen und einen Stellvertreter, die zusätzlich zur Verwaltungstätigkeit in einzelne Arbeitsabläufe der Zertifizierungsstelle eingebunden sein können. Zur Aufrechterhaltung des Betriebes der Infrastruktur sind Systemoperatoren notwendig. Die die Zertifikate betreffende Arbeit der Zertifizierungsstelle wird von Operatoren erledigt, die von einer Person des Sekretariats unterstützt werden. Um jederzeit eine Sperrung eines Zertifikates zu ermöglichen und dabei das Vieraugenprinzip einzuhalten, sind mindestens 9 Personen vorzusehen[481]. Als letztes sei der Wachdienst des Gebäudes erwähnt, der ebenfalls zu jeder Zeit verfügbar sein muß. Bei der Vergabe der Aufgaben und Rollen ist darauf zu achten, daß bestimmte Kombinationen von Aufgaben nicht von einer Person durchgeführt werden dürfen[482].

Es ist möglich, Tätigkeiten des Sperrdienstes nachts auf den Wachdienst und tagsüber auf andere Mitarbeiter der Zertifizierungsstelle zu verlagern. Aus Sicherheitsgründen ist dies jedoch nicht ratsam, da der Wachdienst im Falle eines Sperranrufes seine eigentliche Aufgabe vernachlässigen müßte. Außerdem sollten

[481] 168 Std. pro Woche mit 2 Personen gleichzeitig entspricht bei 38 Std. Arbeitszeit pro Woche einem Bedarf von 8,84 Personen und damit 9 Personen; Krankheiten und Urlaub sind nicht eingerechnet.

[482] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 70.

mindestens zwei Personen an der Protokollierung des Sperreintrages und der Signatur desselben beteiligt sein, um Fehlern und Mißbrauch vorzubeugen[483].

Die Einrichtung eines Call-Centers, um die Sperranträge entgegennehmen zu können, ist sehr kostenintensiv[484], jedoch müssen Anfragen zur Technik, Anwendungen oder Informationen der Teilnehmer beantwortet werden. Aufgrund der besonderen Anforderungen an die Mitarbeiter der Zertifizierungsstelle, exemplarisch seien deren Zuverlässigkeit und Vertrauenswürdigkeit genannt, können Studenten oder Teilzeitkräfte nur bedingt eingesetzt werden, was sich wiederum in höheren Kosten niederschlägt[485].

Die Telefonkosten sind ebenfalls nicht in die Betrachtung einbezogen, da diese von der gewählten Rufnummer abhängen und auf die Teilnehmer verlagert werden können[486].

5.3.2 Variable Kosten einer Zertifizierungsstelle

In diesem Abschnitt werden die Kosten der Prozesse einer Zertifizierungsstelle untersucht. Dabei werden die Bereitstellungskosten der Infrastruktur nicht berücksichtigt, da diese bereits in den fixen Kosten einer Zertifizierungsstelle enthalten sind. Daher handelt es sich bei den Kosten der Prozesse um die variablen Kosten.

In den ersten drei Abschnitten werden die Prozesse der Ausstellung, Sperrung und Prüfung von Zertifikaten untersucht. In den Abschnitten vier und fünf erfolgt die Betrachtung der Erstellung und Prüfung von Zeitstempeln. Im letzen Abschnitt

---

[483] Vgl. Bertsch/Pordesch (Problematik von Prozeßlaufzeiten, 1999), S. 514.

[484] Vgl. Rupp (Call Center Praxis, 2000), S. 67ff und 71ff;
Vgl. o.V. (Investitionskosten beim Aufbau eines Call Centers, 2001), Internet-Quelle.

[485] Vgl. RegTP (BSI-Handbuch für digitale Signaturen, 1997), S. 64;
o.V. (Investitionskosten beim Aufbau eines Call Centers, 2001), Internet-Quelle.

[486] Möglich und teilnehmerfreundlich wäre eine für Teilnehmer kostenlose 0800-Nummer, andere Varianten von 0180/2 – 0190/0 sind ebenfalls denkbar.
Vgl. Deutsche Telekom AG (Servicerufnummern, 2002), Internet-Quelle.

wird der Prozeß der Rechnungsstellung untersucht, dessen Kosten in die eines Zertifikates einfließen müssen.

5.3.2.1 Ausstellung von Zertifikaten

Um als Teilnehmer in den Besitz eines Zertifikates zu gelangen, muß als erstes der Antrag der Zertifizierungsstelle ausgefüllt und an diese übermittelt werden. Neben vollständigen und korrekten Angaben muß zusätzlich die Identität nachgewiesen werden. Hier sind die beiden unterschiedlichen Möglichkeiten des persönlichen Erscheinens des Antragstellers und der Authentifikation durch einen vertrauenswürdigen Dritten zu berücksichtigen. Im Falle eines Fehlers muß Kontakt mit dem Antragsteller aufgenommen werden.

Ist ein Antrag akzeptiert worden, so muß das Zertifikat erstellt, die Chipkarte personalisiert und dem Antragsteller übergeben werden. Wird die Chipkarte versandt, muß die Freischaltung der Karte mittels eines PIN- oder Null-PIN-Verfahrens[487] realisiert werden. Die Zertifizierungsstelle muß Sorge tragen, daß freigeschaltete Zertifikate in das Verzeichnis aufgenommen werden, so daß deren Gültigkeit von Dritten prüfbar ist. Ab der Freischaltung kann der Teilnehmer das Zertifikat verwenden. Der gesamte Vorgang muß dokumentiert werden.

5.3.2.2 Sperrung von Zertifikaten

Die Zertifizierungsstelle muß für die Sperrung von Zertifikaten eine Rufnummer bereithalten, unter der die Teilnehmer eine Sperrung ihres Zertifikates in Auftrag geben können und für diese in diesem Fall Übertragungskosten anfallen. In der hohen Sicherheitsstufe muß dies jederzeit möglich sein, so daß daraus entsprechend hohe Personalkosten resultieren, die sich in den Gesamtkosten niederschlagen. Für eine sichere Abwicklung des Prozesses müssen mindestens zwei Personen

---

[487] Bei dem Null-PIN-Verfahren entfällt die postalische Übersendung von PIN-Briefen, weil die PIN während der erstmaligen Nutzung durch den Anwender generiert wird.
Vgl. BMWi/BMI/BSI (Haushaltswirtschaftssystem auf Basis digitaler Signaturen, 2001), S. 3.

beteiligt sein[488]. Diese lassen sich jedoch durch geeignete Aufgabenverteilungen innerhalb des Personals minimieren, zu nennen wäre eine Verknüpfung der Rolle Pförtner und Sperrantragsannahme[489].

Bei Eingang eines Anrufes muß zunächst die Identität des Anrufers mit Hilfe des dafür vorgesehenen Paßwortes verifiziert werden, bevor die Sperrung in Auftrag gegeben wird. Dabei muß sichergestellt werden, daß ab dem Zeitpunkt des Anrufes bis zum überprüfbaren Sperrvermerk des Zertifikates eine vorher zugesicherte Zeitspanne nicht überschritten wird, weil ansonsten ein eventueller Mißbrauch zu Lasten der Zertifizierungsstelle gehen könnte[490]. Dies bedeutet, daß zum einen das Zertifikat in die nächste veröffentlichte Zertifikatsrevozierungsliste (CRL) aufgenommen werden muß und eine Abfrage mittels des Online-Zertifikatsstatusprotokolls (Online Certificate Status Protocol, OCSP) die Sperrung zurückliefert. Die Sperrung des Zertifikates ist zu dokumentieren.

5.3.2.3 Prüfung von Zertifikaten

Die geringsten Kosten aller mit einem Zertifikat zusammenhängenden Prozesse verursacht die Prüfung eines Zertifikates innerhalb der Zertifizierungsstelle, da dieser Prozeß vollständig automatisiert abläuft. Hierbei kann es sich um Prüfungen über das OCSP-Protokoll oder Abfragen der Revozierungslisten handeln[491]. Die Rechnerkosten und festen Leitungskosten sollen wiederum keine Beachtung finden, da diese unabhängig von der Anzahl der Prüfungen anfallen. Zu berücksichtigen sind aus diesem Grund nur die variablen Leitungskosten, als wichtigste seien hier die Traffic-Kosten einer Anfrage genannt.

---

[488] Vgl. Bertsch/Pordesch (Problematik von Prozeßlaufzeiten, 1999), S. 514.

[489] Hier ist zu berücksichtigen, daß dies zu Lasten des erreichten Sicherheitsniveaus führt, wie in Kapitel 5.2.1.5 beschrieben.

[490] Vgl. Bertsch/Pordesch (Problematik von Prozeßlaufzeiten, 1999), S. 514.

[491] Vgl. Mack (Sperren von Zertifikaten, 2001), S. 465.

5.3.2.4 Dokument mit Zeitstempel versehen

Im Gegensatz zur Ausstellung eines Zertifikates ist die Ausstellung eines Zeitstempels unproblematisch, weil die Zertifizierungsstelle nur das Dokument des Teilnehmers, beziehungsweise den Hashwert des Dokumentes, mit einer Darstellung des aktuellen Datums signieren muß[492]. Es wird deutlich, daß die Zertifizierungsstelle außer dem zu stempelnden Dokument keine weiteren Daten des Teilnehmers benötigt.

Dies trifft jedoch nur zu, sofern die Zertifizierungsstelle gewillt ist, diesen Dienst kostenlos anzubieten, da ansonsten Teilnehmerdaten erhoben werden müssen. Als Zusatzangebot zu einem Zertifikat könnte es eine sinnvolle Maßnahme darstellen, ist jedoch aufgrund der anfallenden Kosten nicht im Interesse der Zertifizierungsstelle, da der Dienst für beliebige Personen ohne Zertifikat ebenfalls verfügbar wäre[493].

Damit ergeben sich für die Zertifizierungsstelle zwei Möglichkeiten. Zum einen dürfen nur Zertifikatsinhaber der Zertifizierungsstelle und Teilnehmer, die ein bestimmtes Kontingent an Zeitstempeln erworben haben, den Zeitstempeldienst nutzen. Zur Sicherung des Zugangs zum Zeitstempeldienst wird eine Legitimation von den Teilnehmern gefordert, die ausgegeben werden muß. Zum anderen kann der Dienst kostenlos angeboten werden. Eine Legitimation der Nutzung kann entfallen, da die einzelnen Zeitstempelvorgänge nicht abgerechnet werden müssen.

Darüber hinaus muß jeder vergebene Zeitstempel der Zertifizierungsstelle protokolliert werden, um im Falle der Kompromittierung des Signaturschlüssels das Vorkommen rückdatierter Zeitstempel auszuschließen[494].

Problematisch für die Zertifizierungsstelle sind die mit der Rechnungsstellung verbundenen Kosten, die weit über dem Preis eines Zeitstempels liegen. Aus die-

---

[492] Vgl. Kapitel 4.3.4.

[493] Falls eine Person über kein Zertifikat verfügt, aber dennoch nachweisen möchte, daß ein bestimmtes Dokument zu einem Zeitpunkt existiert hat.

[494] Vgl. BSI (SigI - Zeitstempel, 1999), S. 12.

sem Grund scheidet der Verkauf einzelner Zeitstempeldienstleistungen unabhängig von Zertifikaten aus.

5.3.2.5 Prüfung von Zeitstempeln

Die Prüfung eines Zeitstempels erfolgt ebenso automatisiert wie die Prüfung eines Zertifikates, darüber hinaus ist sie wesentlich einfacher. Im Gegensatz zu einem Zertifikat wird die Prüfung eines Zeitstempels pro ausgegebenem Zeitstempel seltener vorkommen, da ein Zeitstempel direkt an ein Dokument gebunden ist und dieser Zeitpunkt nicht öfter als einmal kontrolliert werden muß[495]. Wird der Aufwand der Beantragung eines Zertifikates mit eingerechnet, so muß ein Zertifikat deutlich öfter während des Gültigkeitszeitraumes genutzt werden, um für den Teilnehmer einen Nutzen zu bringen.

5.3.2.6 Rechnungsstellung

Als letzter Prozeß, der für die Teilnehmer von außen sichtbar ist, soll die Rechnungsstellung der Zertifizierungsstelle untersucht werden. Da sämtliche Dienste elektronisch geleistet werden, liegen diese Daten geeignet zur automatischen, elektronischen Rechnungsstellung vor. Bevor die Rechnungen von den Teilnehmern bezahlt werden, müssen sie an diese versandt werden, wobei Kosten für die Zertifizierungsstelle entstehen. Geschieht dies per Post, so fallen neben den Druck- und Verpackungskosten für den Umschlag und das Eintüten der Rechnung Kosten für den Transport der Rechnungen an. Für Zertifizierungsstellen mit einer großen Anzahl von Rechnungen pro Monat ist eine elektronische Rechnungsstellung wirtschaftlich. Möglichkeiten wären die elektronische Bereitstellung der Rechnungen oder die Nutzung oder Betreibung eines Rechnungsportals (Billing-Portal), auf dem die Teilnehmer ihre Rechnungen einsehen können.

---

[495] Es kann vorkommen, daß ein Dokument an mehrere Empfänger gesandt wurde und jeder von ihnen den Zeitpunkt verifizieren möchte. Dies sollte jedoch die Ausnahme und nicht die Regel darstellen. Aus diesem Grund wird in Kapitel 5.2.4 davon ausgegangen, daß ein Zeitstempel im Schnitt 1,5 mal verifiziert wird.

Weitere Kosten entstehen durch den Zahlungsverkehr, wobei für die Zertifizierungsstelle ebenfalls mehrere Optionen möglich sind. Die geringsten Kosten entstehen, wenn die Rechnungsbeträge per Lastschrift eingezogen werden können. In diesem Fall können die Lastschriftdaten elektronisch mittels Home Banking Computer Interface (HBCI) oder per Datenträgeraustausch (DTA) der Bank übermittelt werden.

Werden die Gebühren von den Teilnehmern überwiesen, müssen die auf dem Konto eingegangenen Beträge den Teilnehmern zugeordnet werden. Dies ist beispielsweise aufgrund von Tippfehlern oder fehlender Kundennummern nicht vollständig automatisiert möglich, so daß durch diese Arbeiten zusätzlich Kosten entstehen. Die mit Abstand höchsten Kosten entstehen jedoch durch zurückgegebene Lastschriften, bei denen das Teilnehmerkonto über ungenügende Deckung verfügt hat, sowie durch ausgebliebene Überweisungen. In diesen Fällen müssen Mahnungen versandt werden, deren Kosten sich nicht vollständig an die Teilnehmer weitergeben lassen. Dies kann beispielsweise durch eine Überweisung auftreten, die nicht zugeordnet werden kann, so daß fälschlicherweise eine Mahnung versandt wird.

5.3.3 Risikokosten einer Zertifizierungsstelle

Neben den kalkulierbaren Kosten der einzelnen Prozesse einer Zertifizierungsstelle müssen zusätzlich eventuelle Unfälle betrachtet werden, die Kosten verursachen[496]. Beispielsweise muß eine Zertifizierungsstelle für den Schaden eines Dritten haften, den dieser durch fehlerhafte Angaben in einem qualifizierten Zertifikat erlitten hat[497]. Im folgenden Abschnitt wird zunächst die Vorgehensweise zur Ermittlung dieser Kosten hergeleitet und beschrieben, bevor potentielle Kostenursachen genannt werden.

---

[496] Risiken für Zertifizierungsstellen werden u.a. in Hunt (Technological infrastructure for PKI, 2001), S. 1468ff. beschrieben.

[497] Vgl. SigG §11.

5.3.3.1 Vorgehensweise

Die beschriebenen fixen und variablen Kosten werden in dieser Arbeit mit entsprechenden Zu- oder Abschlägen behandelt[498], da das reale Umfeld der Investitionen nicht mit hinreichender Genauigkeit prognostiziert werden kann[499].

Die Risikokosten betreffen daher nur die Risiken während des Betriebs. Aus diesem Grund werden im folgenden bekannte Verfahren der Investitionsrechung nur noch hinsichtlich ihrer Eignung zur Berücksichtigung der Unsicherheit bezüglich möglicher Unfälle einer Zertifizierungsstelle untersucht. Dabei wird die Annahme getroffen, daß wenn keine objektiven, dann zumindest subjektive Eintrittswahrscheinlichkeiten vorliegen, so daß nicht von Ungewißheit, sondern von kalkulierbarem Risiko gesprochen werden kann[500]. Zunächst werden das Korrekturverfahren, die Sensitivitätsanalyse, die betriebswirtschaftliche Risikoanalyse und das Entscheidungsbaumverfahren kurz erläutert, bevor auf Entscheidungsregeln näher eingegangen wird. Aufgrund der dabei dargelegten Schwächen bildet die Beschreibung des verwendeten Verfahrens der Risikoanalyse aus Sicht der Informatik den Abschluß.

Beim Korrekturverfahren werden die geplanten Eingangsdaten einer Investitionsrechnung durch Zu- und Abschläge verändert. Damit wird die Unsicherheit der Erwartungen berücksichtigt, weil die Berechnung von Werten erfolgt, die mit großer Sicherheit erreicht oder sogar übertroffen werden. Aus diesem Grund ist aber der Einsatz des Korrekturverfahrens nicht ratsam, weil der Eintritt eines Schadensfalls unabhängig von der üblichen Geschäftstätigkeit einer Zertifizierungsstelle ist und daher keine Risikozu- oder –abschläge vorgenommen werden können[501].

Ein weiteres Verfahren stellt die Sensitivitätsanalyse[502] dar, bei der Zusammenhänge zwischen den Eingangsdaten und der Ergebnisgröße untersucht werden[503].

---

[498] Siehe Beschreibung des Korrekturverfahrens weiter unten.

[499] Vgl. Betge (Investitionsplanung, 1998), S. 65.

[500] Vgl. Betge (Investitionsplanung, 1998), S. 65.

[501] Vgl. Domschke/Scholl (Grundlagen der Betriebswirtschaftslehre, 2002), S. 258f.

[502] Vgl. Domschke/Drexl (Einführung in Operations Research, 1995), S. 44ff.

[503] Vgl. Betge (Investitionsplanung, 1998), S. 66.

Dabei lassen sich im wesentlichen zwei Fragestellungen unterscheiden. Zum einen, wie weit eine oder mehrere Rechengrößen vom ursprünglichen Wertansatz abweichen dürfen, ohne daß das Ergebnis einen vorgegebenen Wert unterschreitet und damit die Entscheidung falsch wird. Zum anderen, wie sich das Ergebnis im Falle der Abweichung einer oder mehrerer Eingangsdaten vom ursprünglichen Ansatz ändert[504]. Hier gilt, wie beim Korrekturverfahren, daß der Schadeneintritt keine Abweichung von den Eingangsgrößen darstellt, sondern unabhängig davon zu betrachten ist.

Bei der Risikoanalyse, wie sie in betriebswirtschaftlicher Literatur beschrieben wird, wird versucht, eine Wahrscheinlichkeitsverteilung der Ergebnisgröße mittels analytischer Methoden oder Simulation herzuleiten[505]. Diese Analyse eignet sich für eine große Anzahl alternativer Zukunftslagen, beispielsweise im Falle von Investitionsentscheidungen[506]. Diese Situation ist jedoch nicht gegeben, da ein potentieller Schadensfall nur eintreten kann oder nicht eintreten kann. Des weiteren sind die entstehenden Kosten eines Schadensfalls pro Zertifikat oder Jahr zu ermitteln, so daß die Risikoanalyse ebenfalls nicht einzusetzen ist.

Das letzte betrachtete Verfahren, das Entscheidungsbaumverfahren, betrachtet mehrstufig angelegte Prozesse, bei denen Folgeentscheidungen zu treffen sind. Daran wird deutlich, daß ein Einsatz zur Ermittlung der Risikokosten nicht sinnvoll möglich ist[507].

Entscheidungsregeln bei Risiko sollen zum Abschluß betrachtet werden. Sie basieren auf einer vollständigen Datenauswertung. Exemplarisch sind die Bayes-Regel, die μ-σ-Regel als Verbesserung der Bayes-Regel und das Bernoulli-Prinzip[508] zu nennen. Sie basieren darauf, daß die Eintrittswahrscheinlichkeiten der verschiede-

---

[504] Vgl. Domschke/Scholl (Grundlagen der Betriebswirtschaftslehre, 2002), S. 259.

[505] Vgl. Domschke/Scholl (Grundlagen der Betriebswirtschaftslehre, 2002), S. 260.

[506] Vgl. Betge (Investitionsplanung, 1998), S. 74.

[507] Vgl. Domschke/Scholl (Grundlagen der Betriebswirtschaftslehre, 2002), S. 69ff;
Vgl. Betge (Investitionsplanung, 1998), S. 77.

[508] Für weitere Lösungsmöglichkeiten bei Risiko und eine ausführliche Diskussion vgl. Domschke/Scholl (Grundlagen der Betriebswirtschaftslehre, 2002), S. 50ff.

nen Umweltzustände bekannt sind und daß diejenige Alternative zu wählen ist, bei welcher der mathematische Erwartungswert der Ergebnisgröße optimal ist[509]. Aufgrund mangelnder Alternativen kommen Entscheidungsregeln ebenfalls nicht für die Ermittlung der Risikokosten in Betracht[510].

Problematisch bei sämtlichen Verfahren bei Risiko ist, daß Entscheidungen hinsichtlich möglicher Alternativen zu treffen sind oder die Wahrscheinlichkeit von Zuständen bewertet wird. Die zu betrachtenden Risiken haben dabei direkten Einfluß auf die Geschäftstätigkeit. Im Gegensatz dazu müssen bei der Ermittlung der Risikokosten einer Zertifizierungsstelle die Kosten möglicher Unfälle bestimmt werden, um die Gesamtkosten eines Zertifikates berechnen zu können. Aus diesem Grund wird eine Risikoanalyse, wie sie in der Informatik beschrieben wird, verwendet, um die entsprechenden Kosten einschätzen zu können.

Eine Risikoanalyse, beispielsweise bei der Bewertung der Sicherheit einer Firewall, also zum Schutz der eigenen Rechner vor Angriffen durch beliebige Dritte, hat die Bewertung und Reduzierung des möglichen Schadenpotentials zum Ziel[511]. Zu diesem Zweck werden mögliche Bedrohungen im Hinblick auf die Eintrittswahrscheinlichkeit und das Schadenausmaß untersucht. Da sich beide Größen selten exakt ermitteln lassen, erfolgt eine Einteilung in Klassen. Eine Aufteilung in drei Klassen ist ausreichend, weil lediglich die Reihenfolge der zu betrachtenden Bedrohungen von Interesse ist. Diese Reihenfolge bestimmt die Prioritäten der Maßnahmen zur Erhöhung der Sicherheitsniveaus[512]. Eine graphische Darstellung findet sich in Abbildung 5-10.

---

[509] Vgl. Betge (Investitionsplanung, 1998), S. 77-79.

[510] Ebenfalls nicht betrachtet werden aus diesem Grund Lösungsmöglichkeiten bei Ungewißheit, vgl. in diesem Zusammenhang Domschke/Scholl (Grundlagen der Betriebswirtschaftslehre, 2002), S. 53ff.

[511] Vgl. Raepple (Sicherheitskonzepte für das Internet, 2001), S. 9.

[512] Vgl. Teufel/Schlienger (Informationssicherheit, 2000), S. 27f.

Priorität der Maßnahmen		Eintrittswahrscheinlichkeit		
		niedrig	mittel	hoch
Schadenausmaß	niedrig	niedrig	niedrig	mittel
	mittel	niedrig	mittel	hoch
	hoch	mittel	hoch	hoch

Abbildung 5-10 – Tableau einer Risikoanalyse

Im Falle einer Zertifizierungsstelle stellt sich die Situation anders dar. Im Gegensatz zu einer vorhandenen IT-Infrastruktur, die hinsichtlich der Sicherheit verbessert werden soll, müssen bei einer Zertifizierungsstelle mögliche Sicherheitsrisiken bereits beim Aufbau berücksichtigt und entsprechend gewürdigt werden. Daher sollten zumindest die Risiken mit hohem Schadenpotential beseitigt worden sein, je nach Sicherheitsniveau der Zertifizierungsstelle eventuell ebenfalls die Risiken mit mittlerem und niedrigem Schadenpotential. Die verbleibenden Risiken sind jedoch vorhanden und müssen abgeschätzt werden. Sicherheit ist immer relativ und weil hundertprozentige Sicherheit niemals gewährleistet werden kann, ist jederzeit ein Schadenfall denkbar[513].

Eine Einteilung in Klassen ist an dieser Stelle nicht ausreichend. Zur Zeit liegen jedoch noch keine statistischen Daten zur Ermittlung der Eintrittswahrscheinlichkeiten und des Schadenausmaßes vor. Erst damit kann das Schadenpotential in € als Produkt aus Eintrittswahrscheinlichkeit und Schadenausmaß[514] errechnet und

[513] Vgl. Buchmann (Wie sicher kann Sicherheit sein, 2001), S. 1.

[514] Vom Deutschen Institut für Normung (DIN) in der Norm des Verbands der Elektrotechnik (VDE) 31000 beschrieben.

Die mathematische Definition befindet sich auch in Raepple (Sicherheit in elektronischen Märkten, 2002), S. 65.

Ein grundlegende Betrachtung der Risikoanalyse befindet sich in Teufel/Schlienger (Informationssicherheit, 2000), insbesondere S. 26-28.

auf die entsprechenden Prozesse umgelegt werden[515]. Der mit dieser Rechnung ermittelte Wert hat nicht den Anspruch exakt zu sein, bietet jedoch eine Kalkulationsgrundlage. Denn die Größenordnung der Kosten kann ausreichen, um zu entscheiden, ob der Wert bei der Ermittlung der Kosten eines Zertifikates vernachlässigt werden kann oder nicht. Das Schadenpotential eines einzelnen Risikos kann durch folgende Formel berechnet werden[516]:

Schadenpotential = Eintrittswahrscheinlichkeit * Schadenausmaß

Das Schadenpotential stellt somit einen Erwartungswert dar, da für die Gegenwahrscheinlichkeit des Nichteintritts eines Schadens ein Schadenausmaß von 0 € in das Schadenpotential einfließt. Zusätzlich verdeutlicht die Formel die Proportionalität zwischen Schadenpotential und Eintrittswahrscheinlichkeit sowie Schadenpotential und Schadenausmaß.

Des weiteren bringt es Vorteile, sämtliche Risiken zu betrachten, selbst wenn einige bereits durch die Haftpflichtversicherung gedeckt werden und daher die Kosten der Versicherung in die Kalkulation einbezogen werden könnten, denn der Zertifizierungsdiensteanbieter kann mit Hilfe dieser Betrachtungen den Preis der Versicherungspolice beurteilen.

Aus den geschilderten Überlegungen folgt, daß die Ermittlung der Risikokosten durch die Aufsummierung sämtlicher Schadenpotentiale erfolgt. Aufgrund fehlender empirischer Daten erfolgt in dieser Arbeit im Fallbeispiel eine Einteilung in Klassen, während die Ermittlung der Eintrittswahrscheinlichkeiten und Schadenausmaße im Einzelfall in Abhängigkeit der errichteten Zertifizierungsstelle zu vorzunehmen ist.

---

[515] Vgl. Kyas (Sicherheit im Internet, 1998), S. 19.

[516] Vgl. DIN VDE Norm 31000;

Vgl. Kyas (Sicherheit im Internet, 1998), S. 19.

5.3.3.2 Kostenermittlung durch Risikoanalyse

In der Risikoanalyse[517] wird untersucht, welche verbleibenden Risiken zu welchen Schäden führen können[518]. Schäden innerhalb der eigenen Organisation sind durch organisatorische Maßnahmen und Kontrollen auf ein Minimum reduziert, so daß nur noch potentielle Angriffe erörtert werden müssen. Hier sind Angreifer mit dem Wunsch nach persönlicher Bereicherung und solche mit anderen Motiven zu unterscheiden.

Diese Unterscheidung wird anhand der Klassifizierung der Angriffe auf Zertifizierungsstellen aus Kapitel 4.4 durchgeführt. Begonnen wird mit der Kompromittierung eines Teilnehmerzertifikates, im zweiten Abschnitt folgt die Betrachtung der Kompromittierung mehrerer Teilnehmerzertifikate. Im folgenden Abschnitt wird der erwartete Schaden der Kompromittierung des Wurzelzertifikates der Zertifizierungsstelle betrachtet. Im vierten und fünften Abschnitt erfolgt die Analyse der Kompromittierung eines und aller eingesetzten Verfahren. Im letzten Abschnitt werden die Schadenpotentiale von Angriffen gegen die Verfügbarkeit der Dienstleistungen der Zertifizierungsstelle erörtert.

5.3.3.2.1 Kompromittierung eines Teilnehmerzertifikates

Wird ein Teilnehmerzertifikat kompromittiert und daraufhin vom Benutzer gesperrt, so fallen bei der Zertifizierungsstelle Kosten an, die in der Kalkulation des Zertifikatpreises enthalten sein müssen. Sollte ein Mißbrauch des Zertifikates stattgefunden haben, so entsteht dem Teilnehmer ein Schaden, der im Falle eines nachgewiesenen Verschuldens der Zertifizierungsstelle von der Zertifizierungsstelle übernommen wird. Die gesetzlich vorgeschriebene Mindestdeckungsvorsorge beträgt dabei 250.000 €[519].

---

[517] Vgl. Gerber/Solms (From Risk Analysis to Security Requirements, 2001), S. 580;
Vgl. Eckert (IT-Sicherheit, 2001), S. 87;
Vgl. Kyas (Sicherheit im Internet, 1998), S. 20.

[518] Vgl. Eckert (IT-Sicherheit, 2001), S. 102.

[519] Vgl. SigG §12.

Ein Verschulden der Zertifizierungsstelle liegt vor, wenn ein Zertifikat fehlerhafte Angaben enthält oder wenn der Mißbrauch des Zertifikates nach der Sperrung des Teilnehmers und nach Ablauf der Prozeßlaufzeit erfolgt ist und die Prozeßlaufzeit innerhalb akzeptabler Grenzen liegt[520]. Dafür kommen verschiedene Fehlerquellen in Betracht.

Während das vorher genannte Risiko pro ausgegebenem Zertifikat auftritt und damit zu den variablen Kosten zu zählen ist, ist das Risiko der Beantragung eines Zertifikates mit einer unechten Identität von der Anzahl der ausgegebenen Zertifikate unabhängig und damit fix. Des weiteren ist zu bedenken, daß aufgrund des Vorsatzes des Teilnehmers mit einem höheren Schadenausmaß zu rechnen ist als bei einem Fehler der Zertifizierungsstelle, der zufällig ausgenutzt wird.

5.3.3.2.2 Kompromittierung mehrerer Teilnehmerzertifikate

Die Kompromittierung, beziehungsweise der Mißbrauch mehrerer Teilnehmerzertifikate ist aufgrund der Tatsache, daß, anders als bei Kreditkarten, die sensiblen Daten einer Karte nicht mehr ausgelesen werden können, wesentlich erschwert.

Für einen Angreifer, dem der Mißbrauch eines einzelnen Zertifikates nicht ausreicht, wird es demnach schwer, in den Besitz mehrerer gültiger Zertifikate zu gelangen. Jedoch ist festzustellen, daß der niedrigeren Eintrittswahrscheinlichkeit eines Schadenfalls ein höheres Schadenausmaß gegenüber steht.

5.3.3.2.3 Kompromittierung des Wurzelzertifikates

Sollte es einem Angreifer gelingen, das Wurzelzertifikat einer Zertifizierungsstelle zu kompromittieren, erlischt damit die Gültigkeit aller Zertifikate, sofern dies bekannt würde. Der Angreifer wäre in der Lage, beliebige Zertifikate zu erstellen. Sofern der Angreifer den Schlüssel durch einen Brute-Force-Angriff[521] erhalten hat, kann die Zertifizierungsstelle ein neues Schlüsselpaar generieren und mit der

---

[520] Vgl. Bertsch/Pordesch (Problematik von Prozeßlaufzeiten, 1999), S. 514.

[521] Vgl. Schneier (Applied Cryptography, 1996), S. 8.

Ausgabe der neuen Zertifikate an die Teilnehmer beginnen. Sowohl Teilnehmer als auch Zertifizierungsstelle können sämtliche Geräte und Verfahren weiter nutzen.
Ein weiterer möglicher Angriff wäre es, zu versuchen, durch Datenspionage in den Besitz des Wurzelzertifikates zu gelangen, um eigene Zertifikate auszustellen. Bereits das Wissen von einem gefälschten Zertifikat hätte den Vertrauensverlust aller von der Zertifizierungsstelle ausgegebenen Zertifikate zur Folge.

5.3.3.2.4 Kompromittierung eines eingesetzten Verfahrens

Die Risikoanalyse der Kompromittierung eines eingesetzten Verfahrens scheint auf den ersten Blick nicht notwendig zu sein, da die eingesetzten Verfahren mit der Maßgabe ausgewählt werden, daß sie für den gewählten Zeitraum als sicher zu betrachten sind[522]. Durch mathematische Fortschritte oder Neuentwicklungen in der Kryptoanalyse können diese Verfahren jedoch vorzeitig unsicher werden[523]. Aus diesem Grund kann eine Kompromittierung eines Algorithmus nicht vollständig ausgeschlossen werden[524], da die verwendeten Signatur- und Hashverfahren nicht beweisbar sicher sind[525].
Um die Wahrscheinlichkeit der Kompromittierung eines Verfahrens abschätzen zu können, wird exemplarisch das RSA-Verfahren betrachtet. Es basiert auf der Schwierigkeit, große Zahlen zu faktorisieren, das heißt, sie in ihre Primfaktoren zu zerlegen[526]. Schwierigkeit bedeutet hierbei, daß noch kein effizientes Verfahren zur Lösung des Problems gefunden wurde, obwohl Mathematiker bereits seit langer Zeit nach solchen Verfahren suchen[527].
Der Umgang mit Zahlen ist im Gehirn des Menschen ein Prozeß, der durch Übung und Erfahrung ausgebildet wird. Menschen sind damit in der Lage, ihre Fähigkeiten durch Übung zu verbessern. Darüber hinaus verfügen Menschen aufgrund gei-

---

[522] Vgl. Bundesanzeiger (Geeignete Kryptoalgorithmen, 2000).

[523] Vgl. BSI (Signatur-Interoperabilitätsspezifikation, 1999), S. 29.

[524] Vgl. Russell/Cunningham (Maximum Protection, 2001), S. 235.

[525] Vgl. Hartmann/Maseberg (Fail-Safe-Konzepte für FlexiPKI, 2002), S. 1.

[526] Vgl. Buchmann (Einführung in die Kryptographie, 2001), S. 115.

[527] Vgl. ebenda, S. 119.

stiger Behinderung oder autistischer Veranlagung in isolierten Bereichen über hoch entwickelte Fähigkeiten. Als wichtigste zahlenbezogene Fähigkeit sei an dieser Stelle das Benennen von Primzahlen genannt[528]. Aufgrund der Behinderung der getesteten Personen ist eine Abschätzung des Ausmaßes dieses Sachverhaltes schwer zu treffen, da sie ungenügende Informationen geben können. Weiter sei jedoch erwähnt, daß sie über ein hervorragendes Zahlengedächtnis verfügen können, das sie in die Lage versetzt, Zahlen mit bis zu dreihundert Stellen zu wiederholen[529]. Festzustellen ist, daß sie in der Lage sind, Zahlen zu faktorisieren, ohne überhaupt zu wissen, was Faktoren bedeuten. Exemplarisch ist ein Spiel zweier autistischer Zwillinge zu nennen, die sich gegenseitig Primzahlen zuzurufen pflegten[530]. Ein Arzt, dem dies aufgefallen war, griff in das Spiel ein, in dem er ebenfalls eine Primzahl einwarf. Nachdem sie seine Zahl geprüft und nach kurzer Zeit mit einem Lächeln für ausreichend befunden hatten, wurde er als Mitspieler akzeptiert. Während dieses Spiels wurden die genannten Primzahlen immer länger, bis nach einer Stunde zwanzigstellige Zahlen[531] verwendet wurden, wobei die Autisten jeweils fünf Minuten Bedenkzeit pro Zahl benötigten[532]. Dies legt nahe, daß es Verfahren zur Primfaktorzerlegung geben könnte, die lediglich noch nicht bekannt sind[533], obwohl das Problem der Primzahlerkennung von dem der Primfaktorzerlegung getrennt betrachtet werden kann[534]. In Anbetracht der Wichtigkeit eines

---

[528] Vgl. Aster (Neuropsychologische Testbatterie für Zahlenverarbeitung, 2001), S. 11.

[529] Vgl. Davidson/Neale (Klinische Psychologie, 1998), S. 554.

[530] Vgl. Kowol (Primzahlen, 1995), S. 4.

[531] Hier konnte der Arzt die Zahlen nicht mehr überprüfen, da seine Primzahl-Tabelle bei zehn Stellen endete.

[532] Vgl. Davidson/Neale (Klinische Psychologie, 1998), S. 555;
Vgl. Rechenzeitbetrachtung von Faktorisierung und Primzahltest in Bressoud (Factorization and primality testing, 1989), S. 18f.

[533] Vgl. Kowol (Primzahlen, 1995), S. 5.

[534] Vgl. Bressoud (Factorization and primality testing, 1989), S. 70.

solchen Algorithmus und der erhöhten Anstrengungen einen solchen zu finden, ist davon auszugehen, daß dieser letztendlich gefunden wird, sollte er existieren[535].

Aus dieser Darstellung wird deutlich, daß ein Schadensfall auf keinen Fall vollständig ausgeschlossen werden kann, obwohl die Wahrscheinlichkeit sehr gering ist. Aus diesem Grund muß in der Risikoanalyse zwischen einfachen und Fail-Safe-Konzepten von Public-Key-Infrastrukturen unterschieden werden. Die Grundidee dieser Konzepte besteht in der Nutzung unabhängiger und einsatzspezifischer kryptographischer Komponenten, so daß bei der Kompromittierung einzelner Komponenten die Infrastruktur weiterhin sicher funktioniert. Dies ist der Fall, wenn es möglich ist, die kompromittierten Komponenten sicher auszutauschen, elektronische Dokumente mehrfach zu signieren und nicht alle Komponenten gleichzeitig von einem Schadensfall betroffen sind. Äquivalent bedeutet dies, daß weder sämtliche zugrundeliegenden mathematischen Basisprobleme gleichzeitig gelöst werden, noch neue effiziente Lösungsverfahren entwickelt werden und es nicht gelingt, leistungsstarke Rechner[536] zu bauen, die alle kryptographischen Probleme lösen können[537].

Mit dem Einsatz von Fail-Safe-Konzepten[538] wird das potentielle Schadenausmaß im Falle der Kompromittierung damit deutlich reduziert, da die Infrastruktur weiterhin bestehen und benutzbar bleibt[539]. Dieser Vorteil wird durch den erhöhten Aufwand zur Unterhaltung einer solchen Infrastruktur erreicht[540].

---

[535] Zum Vergleich die Dauer des Beweises für Fermat's letzten Satz, den Andrew Wiles nach acht Jahren Arbeit über 300 Jahre nach Stellen der Aufgabe lieferte.
Vgl. Singh (Fermats letzter Satz, 2001), S. 12ff.

[536] Hier sei auf Quantencomputer verwiesen, von denen angenommen wird, daß sie dies könnten.

[537] Vgl. Hartmann/Maseberg (Fail-Safe-Konzepte für FlexiPKI, 2002), S. 2.

[538] In jedem Fall müssen Fail-Stop-Signaturen zum Einsatz kommen.
Vgl. Langenbach/Ulrich (Elektronische Signaturen, 2002), S. 24.

[539] Vgl. Hartmann/Maseberg (Fail-Safe-Konzepte für FlexiPKI, 2002), S. 10;
Vgl. Langenbach/Ulrich (Elektronische Signaturen, 2002), S. 100.

[540] Vgl. Hartmann/Maseberg (Fail-Safe-Konzepte für FlexiPKI, 2002), S. 8.

5.3.3.2.5 Kompromittierung aller eingesetzten Verfahren

Sämtliche Überlegungen werden irrelevant, wenn die Annahmen des Fail-Safe-Konzeptes nicht erfüllt sind und es demnach gelingt, sämtliche Verfahren und Algorithmen gleichzeitig zu kompromittieren. In diesem Fall ist nicht nur die vorhandene Public-Key-Infrastruktur zerstört, zusätzlich kann keine neue Infrastruktur aufgebaut werden.

An dieser Stelle sollte erwähnt werden, daß einem Wissenschaftler, der eines oder alle benutzten Verfahren brechen kann, wahrscheinlich kein Interesse an einer betrügerischen Bereicherung unter Nutzung digitaler Signaturen unterstellt werden kann, da neben dem wissenschaftlichen Ruhm auch finanzielle Vorteile zu erwarten wären. Außerdem sollte sich die Entdeckung nicht lange verheimlichen lassen, da üblicherweise mehrere Forscher an einem Gebiet arbeiten.

Die Wahrscheinlichkeit eines solchen Schadensfalles ist als deutlich geringer einzustufen als der vorher beschriebene, das Schadenausmaß beträfe allerdings sämtliche getätigten Investitionen.

5.3.3.2.6 Angriffe gegen die Verfügbarkeit der Dienstleistungen

Neben der Kompromittierung eines Zertifikates oder eines Verfahrens könnte ein Angreifer versuchen, die Infrastruktur einer Zertifizierungsstelle anzugreifen. Während physische Angriffe durch infrastrukturelle Maßnahmen weitgehend ausgeschlossen sind, stellen die weiter oben beschriebenen Distributed Denial of Service-Angriffe (DDoS) eine größere Gefahr dar, da sie einfacher durchzuführen sind[541]. Dies ist unter anderem darauf zurückzuführen, daß Angreifer nicht über das dazu notwendige Wissen verfügen müssen, sondern auf fertige Skripte oder Baukästen zurückgreifen können[542].

Aus diesem Grund müssen bei der Risikoanalyse die Angriffe gegen die Verfügbarkeit der Dienstleistungen der Zertifizierungsstelle unter verschiedenen Ge-

---

[541] Vgl. Schneier (Secrets & Lies, 2001), S. 177ff.

[542] Vgl. Schmidt (Virenbasteln für Dummies, 2001), S. 99.

sichtspunkten betrachtet werden. Zum einen aus Sicht der ausschließlichen Zerstörung der Verfügbarkeit, zum anderen aus Sicht eines Angreifers, der versucht, daraus einen Vorteil zu erlangen. Obwohl der Angriff in beiden Fällen identisch ist, müssen im letzteren Fall wesentlich mehr organisatorische Anforderungen erfüllt sein, so daß die Wahrscheinlichkeit als geringer einzustufen ist. Andererseits ist das zu erwartende Schadenausmaß in jedem Fall höher, da der Schaden des ersteren Falls ebenfalls auftritt.

5.3.4 Gesamtkosten einer Zertifizierungsstelle

In diesem Abschnitt wird die Ermittlung der Gesamtkosten eines Zertifikates beschrieben, die auf den Zwischenergebnissen der vorherigen Abschnitte beruht. Als erstes müssen die variablen Kosten eines Zertifikates ermittelt werden. Da sämtliche Kosten pro Zertifikat anfallen, sind Annahmen über das durchschnittliche Auftreten der Prozesse pro Zertifikat pro Jahr nötig, beispielsweise die durchschnittliche Anzahl an Zeitstempeln pro ausgegebenem Zertifikat. Mit diesen Annahmen ist eine Berechnung der variablen Kosten eines Zertifikates möglich, die für eine Zertifizierungsstelle pro Ausstellung eines Zertifikates durchschnittlich anfallen.

Die risikobezogenen Kosten einer Zertifizierungsstelle lassen sich in zwei Arten von Kosten, nämlich fixe und variable, unterteilen. Zum einen die variablen Risikokosten, die pro Zertifikat pro Jahr anfallen und sich diesem direkt zurechnen lassen, und zum anderen die fixen Risikokosten, die pro Jahr anfallen, unabhängig von der Anzahl der ausgegebenen Zertifikate. Zertifizierungsstellen unterschiedlicher Sicherheitsniveaus verfügen trotz der unterschiedlichen Sicherheitsvorkehrungen über ähnliche Eintrittswahrscheinlichkeiten eines Schadenfalls, da der Nutzen eines Angriffs auf ein nicht beweisbar sicheres Zertifikat und damit die Wahrscheinlichkeit eines solchen Angriffs geringer ist und die höheren Erfolgschancen eines solchen Angriffs bei gleichen Angriffsmitteln ausgleicht. Aus diesem Grund sind die Risikokosten für Zertifizierungsstellen unterschiedlicher Sicherheitsniveaus vergleichbar.

Werden die Fixkosten einer Zertifizierungsstelle mit in die Stückkosten einbezogen, so müssen diese auf die Anzahl an Zertifikaten umgelegt werden, wie in Kapitel 5.1 bei der Beschreibung der Vollkostenrechnung angegeben.
Daher müssen zunächst die Gesamtkosten der Zertifizierungsstelle berechnet werden, die anschließend durch die Anzahl ausgegebener Zertifikate geteilt werden. Für die Gesamtkosten einer Zertifizierungsstelle innerhalb einer Periode ergeben sich die in Abbildung 5-11 dargestellten Kostenverläufe der Gesamtkosten dreier unterschiedlicher Zertifizierungsstellenmodelle in Abhängigkeit der Anzahl ausgegebener Zertifikate und bei unterstelltem linearen Kostenverlauf.

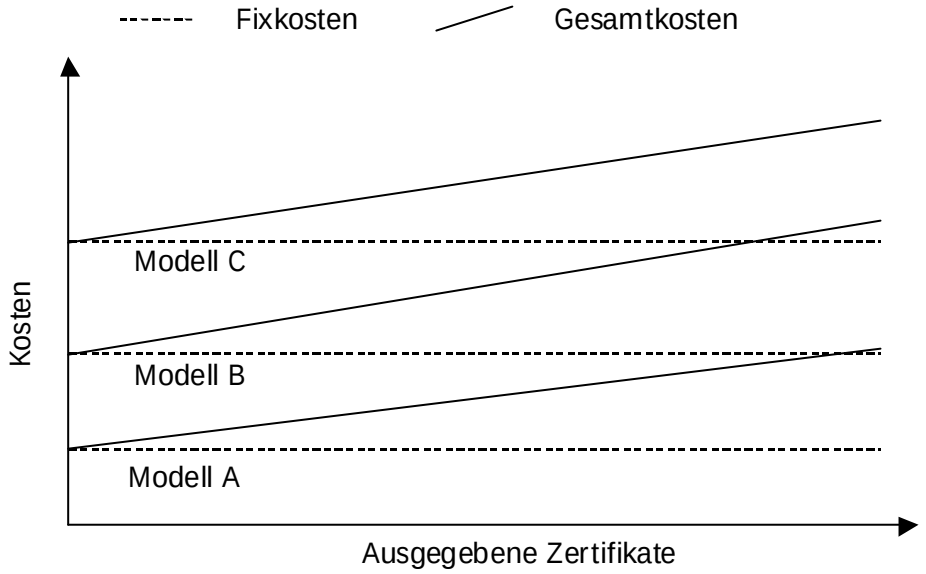

Abbildung 5-11 – Gesamtkosten unterschiedlicher Zertifizierungsstellenmodelle in Abhängigkeit der Anzahl ausgegebener Zertifikate bei unterstelltem linearem Kostenverlauf

Werden die Gesamtkosten der Zertifizierungsstellen der beiden in Kapitel 5.2 vorgestellten Sicherheitsniveaus durch die Anzahl der ausgegebenen Zertifikate geteilt, so nähern sich diese Kosten für große Anzahlen an ausgegebenen Zertifikaten asymptotisch den variablen an[543].

[543] Vgl. Domschke/Scholl (Grundlagen der Betriebswirtschaftslehre, 2002), S. 102ff.

5.4 Erlöse einer Zertifizierungsstelle

Die Erlöse einer Zertifizierungsstelle richten sich nach den kostendeckenden Preisen, die sich für Zertifikate der unterschiedlichen Sicherheitsniveaus erzielen lassen. Da das maximale Sicherheitsniveau durch das Signaturgesetz definiert wurde und Zertifizierungsstellen existieren, die die Anforderungen des Signaturgesetzes erfüllen und daher beweisbar sichere Zertifikate anbieten können, können die entsprechenden kostendeckenden Preise ermittelt werden. Diese Situation liegt bei nicht signaturgesetzkonformen Zertifikaten jedoch nicht vor, so daß keine Aussagen über den kostendeckenden Preis getroffen werden können. Er dürfte den Überlegungen aus Kapitel 4.5 folgend jedoch deutlich unter dem eines signaturgesetzkonformen Zertifikates liegen.
Letztlich bleibt es jedoch dem Anbieter überlassen, für Zertifikate jedes Sicherheitsniveaus einen Preis festzulegen, bei dem er maximalen Gewinn oder Umsatz erwartet.

5.5 Fallbeispiel

Um Aussagen über die Wirtschaftlichkeit einer Zertifizierungsstelle eines signaturgesetzkonformen oder niedrigeren Sicherheitsniveaus treffen zu können, werden in diesem Abschnitt die Kosten der Modelle der minimalen und maximalen Sicherheitsstufe beispielhaft bewertet. Das Fallbeispiel orientiert sich dabei an den in Kapitel 5.3 vorgestellten Modellen. Sämtliche Angaben werden dabei mit Zu- beziehungsweise Abschlägen versehen, um die Risiken zu berücksichtigen. Diese Vorgehensweise entspricht dem in Kapitel 5.3.3.1 beschriebenen Korrekturverfahren, das für die Ermittlung der Risikokosten nicht in Betracht kam, jedoch bei der Ermittlung der fixen und variablen Kosten zur Anwendung kommt. Die angegebenen Werte stellen daher mit großer Sicherheit Schranken für die Kosten dar, so daß den Ergebnissen eine stärkere Aussagekraft zukommt.

Fixe Kosten einer Zertifizierungsstelle

Analog der Systematisierung der Kostenarten in Kapitel 5.3 wird mit den fixen Kosten begonnen.

Aus der Beschreibung des Modells der minimalen Sicherheitsstufe geht hervor, daß ein üblicher Büroraum einschließlich Sicherheitsschrank ausreichend ist. Die Kosten des Raumes richten sich nach dem Standort. Eine Zertifizierungsstelle dieses Sicherheitsniveaus wird nicht als eigenständiges Gebäude errichtet werden, sondern in einem angemieteten Raum eines bestehenden Unternehmens. Die Kosten der Raummiete werden im Einzelfall nach lokalen Gesichtspunkten bestimmt. Die in der Tabelle 5-1 angegebenen jährlichen Kosten des Gebäudes, der Gebäudesicherung und der Energieversorgung für eine minimale Sicherheitsstufe pro Jahr basieren auf einer worst-case Annahme[544].

Wesentlich komplexer ist die Ermittlung der Kosten der Realisierung der maximalen Sicherheitsstufe, die sich an den geschilderten Vorgaben aus Kapitel 3.2.2.1 orientiert. Es muß auf Erfahrungswerte zurückgegriffen werden, die aufgrund der Neuartigkeit der Technik jedoch wenig zahlreich und daher nur bedingt aussagekräftig sind. Die DATEV hat für den Bau ihrer Zertifizierungsstelle den Betrag von 9,5 Millionen € ausgegeben[545], die Kosten der Zertifizierungsstelle der Telekom lagen bei über 25 Millionen €[546] und die Regulierungsbehörde für Telekommunikation und Post geht von Kosten im Bereich zwischen 2,5 und 7,5 Millionen € aus[547]. Als Grundlage der Kostenermittlung dieser Arbeit wird daher ein Betrag

---

[544] Verband Deutscher Makler (Gewerbepreisspiegel 2001, 2001), Internet-Quelle.

[545] Reinhard Muth, DATEV, über Erfahrungen des Zertifizierungsanbieters ZDA-DATEV auf der Tagung Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung am 29.01.2002 in München.

[546] Experteninterview auf der CeBit 2001 mit mehreren Mitarbeitern der Deutschen Telekom.

[547] Vgl. RegTP (Elektronische Signaturen - FAQ, 2002), Frage 6.

von 5 Millionen € angenommen, der deutlich unten dem der Telekom und der DATEV, jedoch in der Mitte der Spanne der RegTP, liegt[548].

Die Gesamtkosten werden unter Annahme eines Zinssatzes von 6% auf 10 Jahre verteilt, so daß jährliche Raten[549] von 680.000 € anfallen. Dazu müssen Nebenkosten und Betriebskosten berücksichtigt werden[550].

Die Hard- und Software muß den Anforderungen aus Kapitel 3.2.2.4 und 5.3.1.2 genügen und die Kapazitätsanforderungen erfüllen.

	Minimale Sicherheit	Maximale Sicherheit
Miete	15.000,00 €	705.000,00 €
Betriebskosten[551]	5.000,00 €	20.000,00 €
Rechner der Mitarbeiter	2.000,00 €	15.000,00 €
Server (Dokumentation, Verzeichnisdienst, Zeitstempeldienst[552])	10.000,00 €	30.000,00 €
Signaturanwendungskomponenten	500,00 €	10.000,00 €
Telekommunikation (Internet-Anschluß, Telefon, Fax, Kopierer)	1.000,00 €	5.000,00 €
Netzwerk		25.000,00 €
Kosten einer Standleitung (redundant 2Mbit)[553]		25.000,00 €

[548] Die RegTP gibt die Kosten einer Zertifizierungsstelle für private Betreiber mit 2,5 – 7,5 Mio € (5-15 Mio DM) an. Die Kosten der Wurzelinstanz betrugen 347.678 € (680.000 DM). Vgl. RegTP (Elektronische Signaturen - FAQ, 2002), Frage 6.

[549] Der Leasingbetrag wird aus Gründen der Vergleichbarkeit mit Miete gleichgesetzt.

[550] Nach einem Expertengespräch mit Herrn Reiner Günther von der VR-Leasing AG.

[551] Beispielsweise Energie, Wasser, Büromaterial und Versicherungen.

[552] Sämtliche Server komplett redundant und zertifizierte Hardware renommierter Anbieter.

[553] Der Datenverkehr einer Zertifizierungsstelle ist gering, weil die Verifikation eines Zertifikates oder eines Zeitstempels aus wenigen kBytes bestehen und die Webseiten zum Auffinden von Zertifikaten so gestaltet werden können, daß der Datenverkehr minimiert wird.
Die Preise für Standleitungen fallen durch die Überkapazitäten und Insolvenzen großer Anbieter ständig. Vgl. n-tv (WorldCom beantragt Insolvenz, 2002), Internet-Quelle und n-tv (KPNQwest: Konkurs angemeldet, 2002), Internet-Quelle.

Unternehmensleiter (Bei minimaler Sicherheit zusätzlich für den Sperrdienst zuständig)	90.000,00 €	90.000,00 €
Systemingenieure (davon einer Stellvertreter) (Bei maximaler Sicherheit 3 Personen)	80.000,00 €	240.000,00 €
Sekretariat		75.000,00 €
Operatoren (3 Personen)		210.000,00 €
Sperrdienst (2 Personen ständig anwesend, insgesamt 9)		500.000,00 €
Wachdienst		200.000,00 €
Kapitalkosten[554]	8.140,00 €	129.000,00 €
Fixkosten der Zertifizierungsstelle	211.640,00 €	2.279.000,00 €

Tabelle 5-1 - Fixkosten des Modells einer minimalen und maximalen Sicherheitsstufe pro Jahr

Variable Kosten einer Zertifizierungsstelle

Nach den fixen Kosten werden im folgenden die variablen Kosten betrachtet. Daher werden, wie im Kapitel 5.3.2 beschrieben, die Prozesse der Erstellung, Sperrung und Prüfung eines Zertifikates, der Erstellung und Prüfung eines Zeitstempels sowie die Kosten der Rechnungsstellung betrachtet[555].

Die geringsten Kosten aller mit einem Zertifikat zusammenhängenden Prozesse verursacht die Prüfung eines Zertifikates innerhalb der Zertifizierungsstelle, da dieser Prozeß vollständig automatisiert abläuft. Hierbei kann es sich um online Prüfungen über das OCSP-Protokoll oder Abfragen der Revozierungslisten handeln[556]. Die Rechnerkosten und festen Leitungskosten sind in den Fixkosten enthalten, da diese unabhängig von der Anzahl der Prüfungen anfallen. Zu

[554] Die anfallenden Kosten müssen, entsprechend der minimalen Sicherheitsstufe, durch die liquiden Mittel für ein halbes Jahr gedeckt sein. Für das gesamte Eigenkapital wird eine Verzinsung von 8% verlangt.

[555] Eine Übersicht über die genauen Arbeitsabläufe ist RegTP (BSI-Handbuch für digitale Signaturen, 1997) zu entnehmen.

[556] Vgl. Mack (Sperren von Zertifikaten, 2001), S. 465.

berücksichtigen sind aus diesem Grund nur die variablen Leitungskosten, als wichtigste seien hier die Traffic-Kosten einer Anfrage genannt.

	Minimale Sicherheit	Maximale Sicherheit
Beantragung eines Zertifikates		
Beantragung eines Zertifikates in der Zertifizierungsstelle	1,00 €	
Beantragung eines Zertifikates auf dem Postweg mittel Post-Ident 3 Verfahren (Staffelpreise ab 25.000, sonst bis 6,49 €[557])		5,44 €
Zertifikat erstellen inkl. Personalisierung des Trägermediums	10,00 €	10,00 €
Starter-Kit, PIN/Null-PIN-Verfahren und Dokumentation (Maximal: Versand)	6,00 €	9,00 €
Signatursoftware für 20.000 Zertifikate[558]	100.000,00 €	100.000,00 €

Übertragungskosten		
Kosten der Sperrung pro 20.000 Zertifikate[559]	2.000,00 €	2.000,00 €
Sperrlistenabruf oder OCSP-Prüfung pro 20.000 Zertifikate	250,00 €	250,00 €
Legitimation zur Nutzung des Dienstes pro 20.000 Zertifikate	5,00 €	5,00 €

[557] Vgl. Deutsche Post (Post-Ident 3, 2001), Internet Quelle.

[558] Die Erstellung einer Software für Zertifizierungsstellen und für die Teilnehmer ist komplex und von der zu betrachtenden Infrastruktur der Zertifizierungsstelle abhängig. Aufgrund des beträchtlichen Risikos einer Individualentwicklung wird von dem Kauf einer Software ausgegangen, bei der kein einmaliger Kaufpreis anfällt, sondern Lizenzgebühren pro erstelltem Zertifikat fällig werden. Aufgrund der am Markt vorhandenen Anbieter von Softzertifikaten ist von Kosten in Höhe von etwa 5 € pro Zertifikat auszugehen, entsprechend den Preisen für reine E-Mail-Zertifikate, exemplarisch sei der Preis von einem T-Online-E-Mail-Zertifikat genannt, der bei 7,60 Euro liegt, vgl. o.V. (T-Online secureMail, 2002), Internet-Quelle.
Die benötigte Funktionalität wird beispielsweise von der Software FlexiPKI erfüllt. Siehe Lehrstuhl Theoretische Informatik, TUD (FlexiPKI, 2001), Internet-Quelle.

[559] In der vorliegenden Arbeit wird davon ausgegangen, das der Sperrvorgang dem Benutzer auf postalischem Weg mitgeteilt wird.

Erstellung von 20.000 Zeitstempeln samt Protokoll	5,00 €	5,00 €
Kosten der Prüfung von 20.000 Zeitstempeln	2,00 €	2,00 €

Rechnungsstellung		
Kosten der Rechnungserstellung	0,01 €	0,01 €
Kosten des Rechnungsversandes pro Rechnung (Post)		1,00 €
Kosten des Lastschrifteinzugs pro 20.000 Lastschriften		0,01 €
Kosten der Fehler beim Lastschrifteinzug (0,1% der Zertifikate)		5,00 €
Kosten der Kontrolle des Zahlungseingangs pro Überweisung		1,00 €
Kosten eventueller Mahnungen (1% der Zertifikate)		5,00 €
Kosten Zahlungsausfall (0,01% der Zertifikate)		150,00 €
Variable Kosten eines Zertifikates bei unterstellter dreijähriger Vertragsdauer pro Jahr	6,06 €	8,87 €

Tabelle 5-2 – Variable Kosten eines Zertifikates

Risikokosten einer Zertifizierungsstelle

Nach den fixen und variablen Kosten einer Zertifizierungsstelle werden zuletzt die Risikokosten betrachtet. Aufgrund fehlender empirischer Daten können diese nicht berechnet werden, sondern sind im Einzelfall unter Berücksichtigung der gewählten Realisierung der Zertifizierungsstelle zu schätzen.

Eine zuverlässige, statistisch signifikante Ermittlung der Eintrittswahrscheinlichkeiten und der entsprechenden Kosten scheidet aus, weil die statistische Masse an vorhandenen Daten fehlt. In der Tabelle 5-3 folgen daher Beispiele, um erfahrungsbegründete, subjektive Aussagen über die in Kapitel 5.3.3 beschriebenen Formen von Angriffe auf Zertifizierungsstellen geben zu können. Die Bewertung von Eintrittswahrscheinlichkeiten und Kosten wird über eine qualitative Skalierung niedrig, mittel und hoch vorgenommen, wie in Kapitel 5.3.3.1 beschrieben. Die angegebene Eintrittswahrscheinlichkeit gibt dabei die geschätzte Wahrscheinlichkeit eines Fehlers pro Vorgang oder die geschätzte Wahrscheinlichkeit eines

Fehlers pro Zertifikat an, sofern es sich um Störfälle und keine regulären Vorgänge der Zertifizierungsstelle handelt.

	Eintrittswahrscheinlichkeit	Kosten
Fehlerhafte Angaben in einem Zertifikat	Hoch	Niedrig
Fehler bei der Annahme des Sperrantrages[560]	Hoch	Niedrig
Fehler bei der Übermittlung der Sperrdaten	Hoch	Niedrig
Fehler beim Sperren des Zertifikates	Hoch	Niedrig
Fehler bei der Online-Statusabfrage eines Zertifikates	Niedrig	Mittel
Fehler bei der Erstellung der Sperrliste	Niedrig	Mittel
Fehler bei Verteilung der Sperrliste	Niedrig	Mittel
Beantragung eines Zertifikates mit einer unecht. Identität[561]	Mittel	Hoch
Mißbrauch bei der Annahme von Sperrungen	Niedrig	Mittel
Mißbrauch bei der Übermittlung von Sperrdaten	Niedrig	Mittel
Kompromittierung des Wurzelzertifikates	Niedrig	Mittel
Erstellen eines gefälschten Zertifikates	Niedrig	Mittel
Kompromittierung eines Verfahrens (mit Fail-Safe-Konzept)	Niedrig	Mittel
Kompromittierung eines Verfahrens (ohne Fail-Safe-Konz.[562])	Niedrig	Mittel
Kompromittierung aller Verfahren	Niedrig	Hoch
Physische Anschläge auf die Infrastruktur	Niedrig	Mittel
Keine Verfügbarkeit der Sperrlisten[563]	Niedrig	Mittel
Keine Verfügbarkeit der Online-Status-Prüfung	Niedrig	Mittel
Zufälliger Mißbrauch von Verfügbarkeitsproblemen	Niedrig	Mittel

Tabelle 5-3 –Risiken einer Zertifizierungsstelle samt Eintrittswahrscheinlichkeiten und entstehenden Kosten

[560] Vgl. Mack (Sperren von Zertifikaten, 2001), S. 465.

[561] Vgl. Mack (Sperren von Zertifikaten, 2001), S. 464.
Einen erfolgten Vorfall beschreibt Bager (Microsoft warnt vor Cracker-Zertifikat, 2001), Internet-Quelle.

[562] Es ist zu beachten, daß für die Teilnehmer im Schadensfall mehr Zeit aufzuwenden ist, um die eigene Infrastruktur wiederherzustellen. Außerdem können ungültig gewordene Signaturen nicht erneuert werden, so daß nur die erneute Signierung zum aktuellen Datum vorgenommen werden kann.

[563] Als exemplarischer Angriff sei eine DDoS-Attacke genannt.

Gesamtkosten einer Zertifizierungsstelle

Die variablen Kosten eines Zertifikates pro Jahr bei dreijähriger Vertragsbindung sind zusammen mit den fixen Kosten Tabelle 5-4 zu entnehmen. Zu beachten ist, daß in diesen Kosten die risikobezogenen Kosten einer Zertifizierungsstelle noch nicht enthalten sind.

	Minimale Sicherheit	Maximale Sicherheit
Fixkosten pro Jahr	211.640,00 €	2.279.000,00 €
Variable Kosten eines Zertifikates	6,06 €	8,87 €

Tabelle 5-4 - Variable Kosten bei dreijähriger Vertragsbindung und Fixkosten eines Zertifizierungsstelle

Um die Gesamtkosten eines Zertifikates beurteilen zu können, muß die Anzahl verkaufter Zertifikate feststehen, um die fixen Kosten auf die Kosten eines Zertifikates umlegen zu können. Dies wird durch Abbildung 5-12 verdeutlicht, in der verschiedene Teilnehmerzahlen angegeben sind. Weiter wird ersichtlich, daß die Anzahl ausgegebener Zertifikate einer Zertifizierungsstelle des minimalen und des maximalen Sicherheitsniveaus bei mindestens 25.000 liegen muß, damit die Fixkosten gedeckt werden.

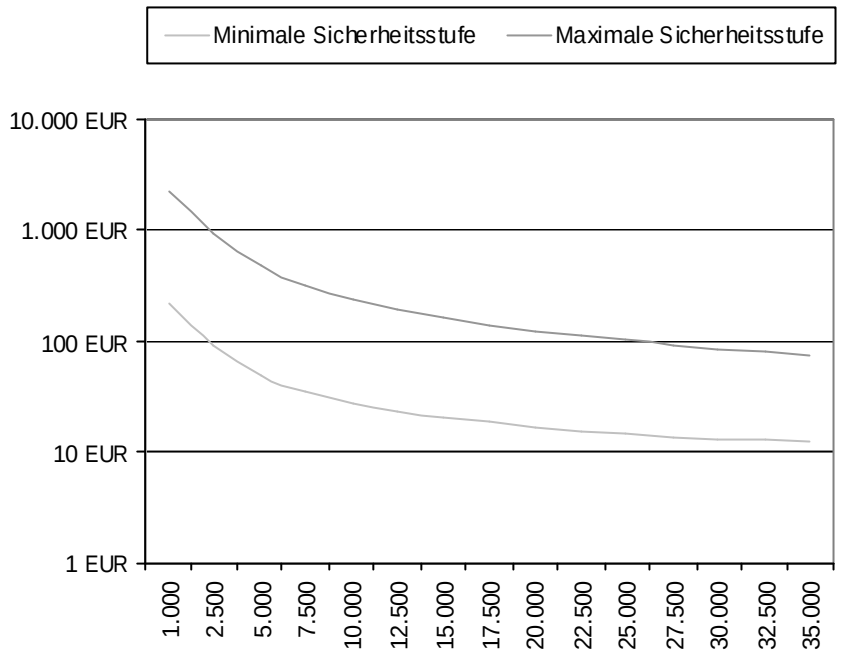

Abbildung 5-12 – Durchschnittskosten eines Zertifikate in Abhängigkeit der Teilnehmerzahl bei minimaler und maximaler Sicherheitsstufe

5.6 Betrachtung der Wirtschaftlichkeit einer Zertifizierungsstelle

Um die Wirtschaftlichkeit einer Zertifizierungsstelle zu beurteilen, müssen im letzten Schritt die Kosten des Fallbeispiels den Erlösen gegenübergestellt werden.

Zusätzlich müssen Annahmen über die erwartete Stückzahl getroffen werden, um die Kosten eines Zertifikates für eine Zertifizierungsstelle abschätzen zu können. Signtrust gab bei der Schließung bekannt, 3.000 Kunden gewonnen zu haben[564], Baltimore verkaufte trotz Erwartungen von 50.000-80.000 nur 1.200 Zertifikate[565] und Telesec spricht von 20.000 Zertifikaten für die digitale Signatur[566]. Diese Zahlen liegen deutlich unter den notwendigen Stückzahlen, um aufgrund der Fixko-

[564] Vgl. Gerbich (Signtrust wird aufgelöst, 2002), Internet-Quelle.

[565] Vgl. Gerbich (Nicht signiert, sondern resigniert, 2002), Internet-Quelle.

stendegression[567] ein marktfähiges Preisniveau zu erreichen, wie im Fallbeispiel in Kapitel 5.5 gezeigt. In dieser Untersuchung wird daher eine Stückzahl von 20.000 angenommen, die das erste Unternehmen am Markt, die Telesec (Deutsche Telekom AG), erreicht hat. Der Preis dieser Zertifikate liegt bei 58,95 €[568].

Wird von diesem Verkaufspreis der kostendeckende Preis für 20.000 Zertifikate in Höhe von 122,82 € abgezogen, so ergibt sich eine Unterdeckung von 63,87 € pro Zertifikat. Daher ist der wirtschaftliche Betrieb einer Zertifizierungsstelle des maximalen Sicherheitsniveaus nicht zu realisieren[569].

Im Gegensatz dazu betragen die Kosten eines Zertifikates des minimalen Sicherheitsniveaus bei vergleichbarer Teilnehmerzahl nur 16,64 €. Damit liegen die Kosten bei 13,55% der Kosten eines Zertifikates der hohen Sicherheitsstufe[570].

---

[566] Vgl. o.V. ("Aus" des TrustCenter-Geschäftes bei der POST AG, 2002), Internet-Quelle.

[567] Vgl. Jahnke (Erfahrungskurve, 2002), Sp. 386.

[568] Dieser Preis ergibt sich bei unterstellter dreijähriger Vertragsbindung. Der Preis eines Signtrust-Zertifikates der Deutschen Post AG liegt mit 37,49 € deutlich unter dem der Telesec. Da die Deutsche Post AG jedoch angibt, Signtrust aufgrund des nicht wirtschaftlichen Betriebes zu schließen, wird der Preis des Signtrust-Zertifikates nicht weiter berücksichtigt. Vgl. Wilkens (Deutsche Post ohne Online-Geschäft, 2002), S. 43.

[569] Der Nutzen eines Zertifikates für einen Teilnehmer muß dessen Kosten übersteigen, vgl. Fox (Zurück auf dem Boden, 2001), S. 442. Um den Nutzen für die Teilnehmer zu erhöhen und damit die Attraktivität von Zertifikaten dieser Sicherheitsstufe zu steigern, müssen erst zusätzliche Anwendungsfälle und zusätzliche Anreize zur Nutzung der bestehenden geschaffen werden. Denkbar wäre beispielsweise eine Weitergabe von Kosteneinsparungen bei Prozessen an Teilnehmer, die bei der Umstellung auf vollständige, elektronischer Abwicklung erzielt werden. Vgl. Krempl (Signatur Schlamassel, 2002), S. 47.

[570] 16,64 € / 122,82 € = 13,55%.

6 Sicherheitsstufen für Zertifizierungsstellen

Aufgrund der durchgeführten Überlegungen stehen die Kosten für die Erstellung von Zertifikaten der minimalen und maximalen Sicherheitsstufe fest. Es wird deutlich, daß die Kosten der maximalen Sicherheitsstufe den zur Zeit erzielbaren Nutzen der Teilnehmer bei weitem übersteigen und aus diesem Grund keine Anreize zur Nutzung vorliegen.

Daher wird in diesem Kapitel zunächst die Vorgehensweise zur Bildung von Sicherheitsstufen für Zertifizierungsstellen dargelegt, bevor diese im zweiten Abschnitt mit Hilfe des Kosten-Sicherheits-Verhältnisses ermittelt werden. Im dritten Abschnitt erfolgt eine Auswahl der Sicherheitsstufen[571], bevor zum Abschluß das Ergebnis der erhaltenen Stufen betrachtet und eine mögliche Vorgehensweise zur breiten Einführung am Markt vorgestellt wird.

6.1 Vorgehensweise zur Bildung der Sicherheitsstufen

Nach den im vorigen Kapitel durchgeführten Überlegungen können aus technischer Sicht viele Zertifizierungsstellen realisiert werden, die sich hinsichtlich der Beweiskraft und Kosten der ausgestellten Zertifikate unterscheiden. Abbildung 6-1 veranschaulicht diesen Sachverhalt, in der auf der horizontalen Achse die Beweiskraft und auf der vertikalen Achse die Kosten der ausgestellten Zertifikate aufgetragen sind. Jeder Kreis symbolisiert ein mögliches Modell einer Zertifizierungsstelle.

[571] Vgl. Fox (Zurück auf dem Boden, 2001), S. 442.

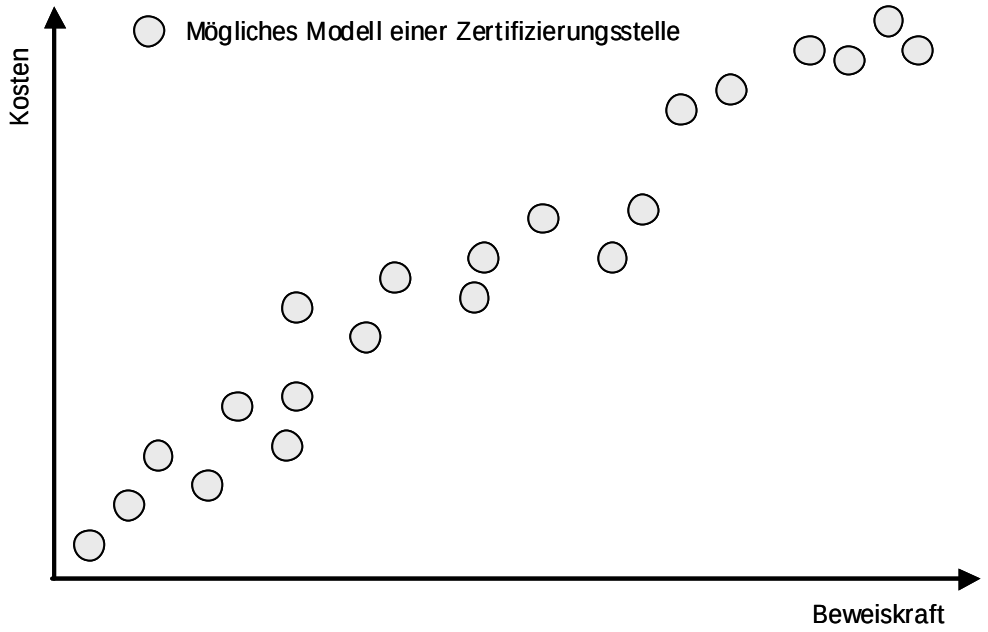

Abbildung 6-1 – Unterschiedliche Beweiskraft und Kosten von Zertifikaten

Während bei zwei unterschiedlichen Modellen von Zertifizierungsstellen, die sich auf der gleichen horizontalen Position befinden die Entscheidung leicht zugunsten des kostengünstigsten Modells getroffen werden kann, kommt bei unterschiedlicher horizontaler Position die Gewichtung der Sicherheit gegenüber den Kosten ins Spiel. Um diese Gewichtung objektiv bewerten zu können, kommt das neu entwickelte Kosten-Sicherheits-Verhältnis in Betracht, welches eine objektive Gewichtung der Sicherheit gegenüber den damit zusammenhängenden Kosten ermöglicht[572].

Um anhand des Kosten-Sicherheits-Verhältnisses Zertifizierungsstellen unterschiedlicher Sicherheitsstufen einteilen zu können, müssen die verschiedenen Teilaspekte getrennt nach dem Kosten-Sicherheits-Verhältnis bewertet werden. Außerdem muß als letzter Teilaspekt die Bewertung der Sicherheit eines Teilnehmers untersucht werden, da die sichersten Zertifikate durch unsachgemäße Nutzung kompromittiert werden können. Hier gilt es, einen geeigneten Kompromiß zu finden. Zum Abschluß erfolgt eine Konsolidierung sämtlicher Teilaspekte.

[572] Vgl. hierzu Kapitel 4.2.3.

6.2 Anwendung des Kosten-Sicherheits-Verhältnisses

Um die verschiedenen, hinsichtlich des Kosten-Sicherheits-Verhältnisses besten Modelle für Zertifizierungsstellen auszuwählen, werden im folgenden die unterschiedlichen Bereiche einer Zertifizierungsstelle einzeln betrachtet.

Neben dem Kosten-Sicherheits-Verhältnis der Zertifizierungsstelle, das sich aus den Teilaspekten Gebäude, Gebäudesicherung, Energieversorgung, Hardware und Software und Personal zusammensetzt, wird zusätzlich das Kosten-Sicherheits-Verhältnis der Teilnehmer betrachtet. Dies ermöglicht eine Einschätzung des tatsächlich erreichten Sicherheitsniveaus digitaler Signaturen, da eine einseitige Betrachtung der Zertifizierungsstelle nur der theoretischen Sicherheit entsprochen hätte[573].

[573] Vgl. Zusammenhang in Schneier (Secrets & Lies, 2001), S. 387.

Bei der Betrachtung des Kosten-Sicherheits-Verhältnisses des Gebäudes ergeben sich zwei Klassen, die in Abbildung 6-2 dargestellt sind. Zum einen eine Klasse, die zumindest ein minimales Sicherheitsniveau erreicht, und bei der die minimalen Anforderungen des Gebäudes aus dem Kapitel Kostenbetrachtung realisiert werden. Die andere Klasse ergibt sich aus den maximalen Anforderungen, da jede Erhöhung einer Sicherheitsmaßnahme auf einem Gebiet ohne eine parallele Erhöhung der korrespondierenden Maßnahmenbündel wirkungslos bleibt. Exemplarisch sei die Abstrahlsicherheit ohne einhergehende Verstärkung der Wände und Türen genannt. Daher sind weitere Klassen nach dem Kosten-Sicherheits-Verhältnis nicht sinnvoll, da beispielsweise den Kosten der Erhöhung des Sicherheitsniveaus von Modell 3 kein entsprechenden Gewinn an Sicherheit gegenübersteht und Modell 5 mit geringen Kosten auf das Sicherheitsniveau von Modell 6 gebracht werden kann.

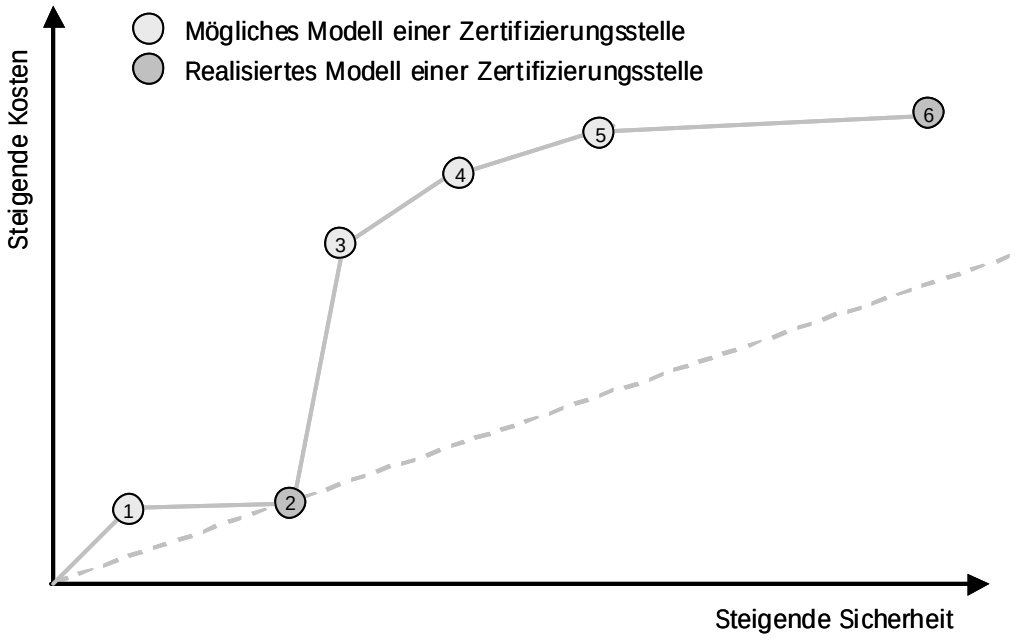

Abbildung 6-2 – Modelle einer Zertifizierungsstelle des Teilaspekts Gebäude

Bei der Gebäudesicherheit ergibt sich ein anderes Bild. Ausgehend von einem minimalen Sicherheitsniveau, bestehend aus Brandschutz und Alarmanlage, kann die Sicherheit durch einzelne Komponenten schrittweise erhöht werden, jeweils ohne besondere Kosten zu verursachen. Als Beleg dafür seien Bewegungsmelder genannt, die die Sicherheit des Gebäude wesentlich erhöhen, aber keinesfalls kostenintensiv sind. Daraus ergeben sich viele Klassen, die alle über ein ähnliches Kosten-Sicherheits-Verhältnis verfügen. Erst durch den Einsatz von Überwachungskameras und Wachpersonal ergibt sich ein anderes Kosten-Sicherheits-Verhältnis, daß für die hohe Sicherheitsstufe jedoch unumgänglich ist. Ob, wie in der Veranschaulichung dieser Modelle in Abbildung 6-3, Modell 2 oder eventuell Modell 4 für das niedrige Sicherheitsniveau gewählt wird, hängt von den erreichten Sicherheitsniveaus der anderen Teilaspekte ab.

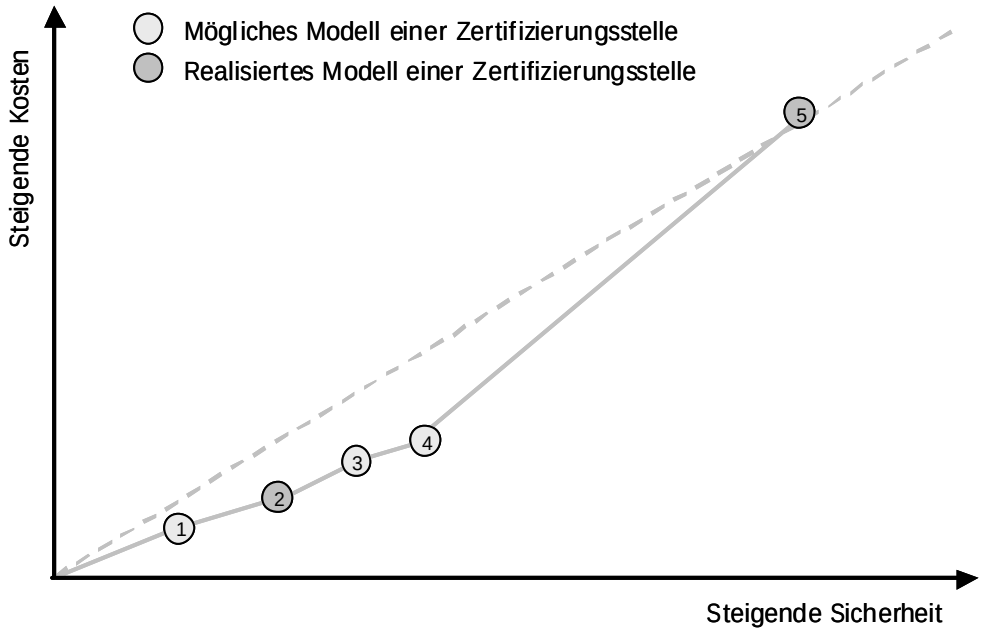

Abbildung 6-3 - Modelle einer Zertifizierungsstelle des Teilaspekts Gebäudesicherheit

Die Energieversorgung der Zertifizierungsstelle ist für die Anforderung der Verfügbarkeit der Leistung unabdingbar. Während die Minimalforderung die Überbrückung eines kurzfristigen Stromausfalls darstellt, können die Anforderungen von einigen Stunden sukzessive nahezu unbegrenzt erhöht werden. Da bereits im Bereich mehrerer Stunden der benötigte Strom nur noch durch eine netzunabhängige Energiequelle, beispielsweise einen mit Treibstoff betriebenen Generator, geliefert werden kann, ergeben sich neben der niedrigsten eine mittlere Klasse, die wenige Stunden überbrücken kann und eine hohe, die für unbegrenzten Betrieb steht. Die entsprechenden Modelle sind in Abbildung 6-4 dargestellt.

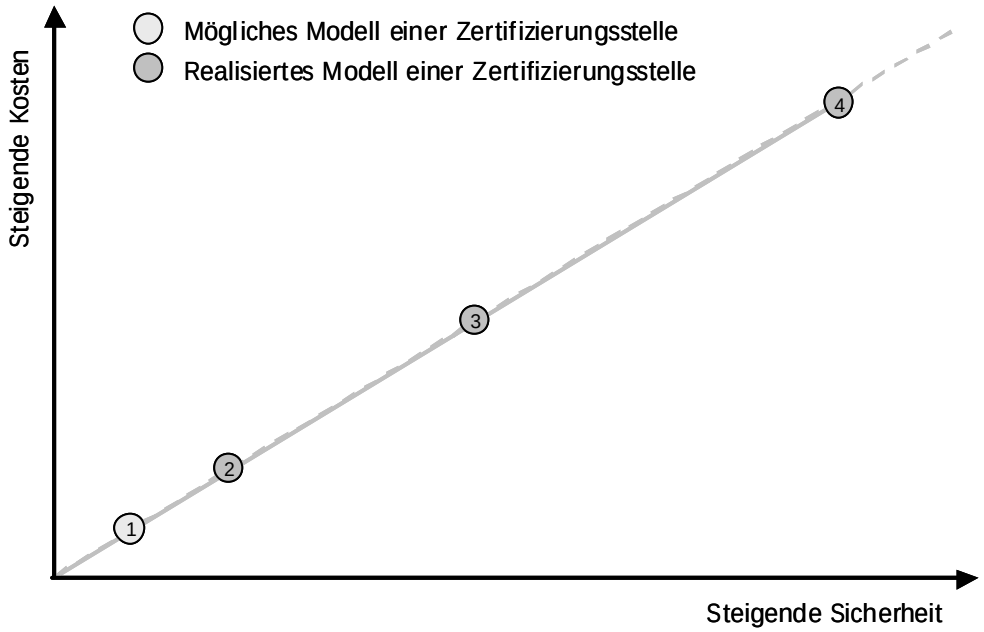

Abbildung 6-4 - Modelle einer Zertifizierungsstelle des Teilaspekts Energie

Wie bereits weiter oben erwähnt, muß die Sicherheit der Software auf jeden Fall gewährleistet sein und läßt sich im Hinblick auf die Funktionalität nicht durch zusätzliche Kosten erhöhen. Höchstens aufgrund durchgeführter Zertifizierungen zum Nachweis des erreichten Sicherheitsniveaus fallen zusätzliche Kosten an. Neben der Klasse niedrig existiert daher eine Klasse, die ein hohes Sicherheitsniveau darstellt. Die Klasse Null entspräche einer unorganisierten Implementierung ohne Konzept und Struktur, bei der keine Wartung möglich wäre. Es wird vorausgesetzt, daß die Software über Fail-Safe-Funktionalität verfügt, da unter Einbeziehung der Kosten eines möglichen Schadensfalls identische Sicherheitsniveaus zu geringeren Kosten realisiert werden, als ohne Fail-Safe-Funktionalität. Eine graphische Übersicht der Modelle findet sich in Abbildung 6-5.

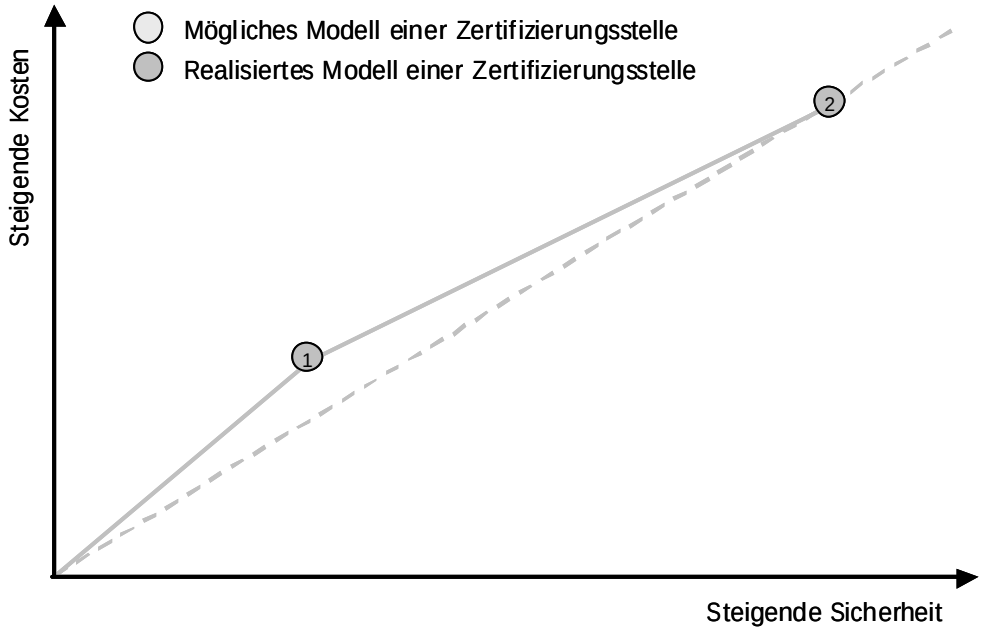

Abbildung 6-5 - Modelle einer Zertifizierungsstelle des Teilaspekts Software

Bei der Betrachtung des Teilaspektes Hardware kann zunächst die Installation der Software auf einem handelsüblichen Rechner und ein Einsatz entsprechend preiswerter Signaturkomponenten vorausgesetzt werden. Nächst höhere Klassen ergeben sich durch den Einsatz redundanter Komponenten und sichererer Hardware, die beispielsweise die Abstrahlung der Hardware reduzieren beziehungsweise vollständig verhindern. Durch die Abspaltung des Verzeichnis- und Zeitstempeldienstes in separate Systeme kann die Sicherheit deutlich gesteigert werden, jedoch erhöht sich der Bedarf an Hardware und damit die Kosten deutlich. Damit ist das Sicherheitsniveau der Klasse hoch auf jeden Fall erreicht, dargestellt durch Modell 9 in Abbildung 6-6. Für die Klassen niedrig und mittel werden die Modelle 2 und 5 gewählt.

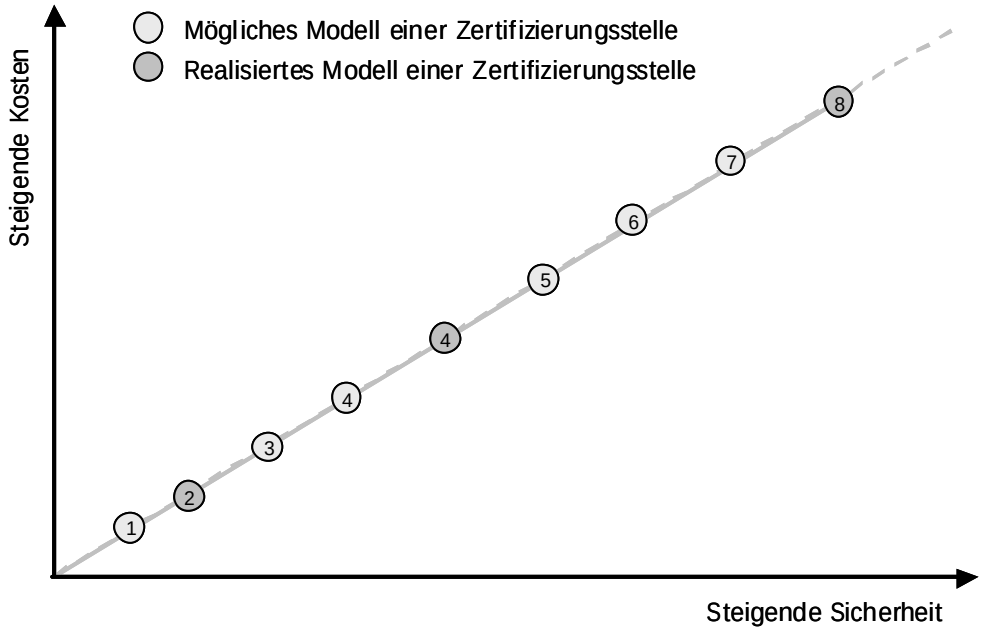

Abbildung 6-6 - Modelle einer Zertifizierungsstelle des Teilaspekts Hardware

Wie bereits im Kapitel Kostenbetrachtung gezeigt, stellen die Personalkosten den wesentlichen Kostenfaktor dar. Aus diesem Grund ergeben sich in diesem Teilaspekt viele Klassen, die sich hinsichtlich des erreichten Sicherheitsniveaus und der Kosten erheblich unterscheiden. In der niedrigsten Klasse kann die Aufgabe des Sperrdienstes auf bestimmte Zeiten eingeschränkt werden, während dieser in der mittleren Klasse unter anderem auf den Wachdienst verlagert werden kann und damit zu einer kostengünstigeren Lösung führt. Eine Erhöhung der Sicherheit ergibt sich im folgenden durch jede Hinzunahme eines weiteren Mitarbeiters, jedoch hat dies entsprechende Kostensteigerungen zur Folge. Gerade im Bereich der hohen Sicherheitsniveaus wird eine Policy, die für sicherheitskritische Vorgänge das Vier-Augen-Prinzip vorschreibt, zwingend notwendig sein. Dadurch verdoppeln sich die Personalkosten dieser Aufgaben. Anschaulich finden sich die dargestellten Modelle in Abbildung 6-7.

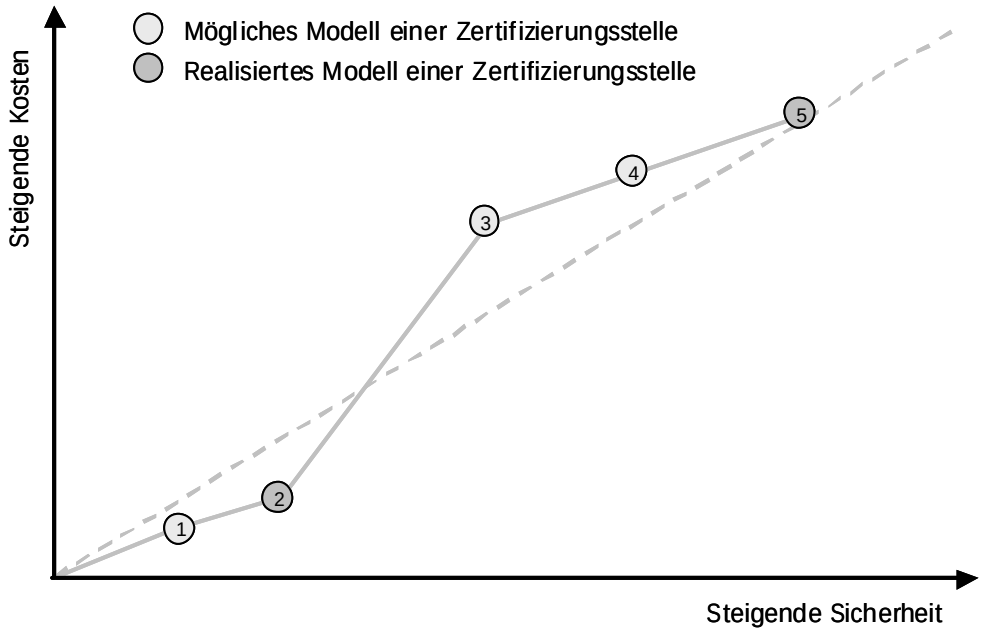

Abbildung 6-7 - Modelle einer Zertifizierungsstelle des Teilaspekts Personal

Als letzter Punkt ist der Teilaspekt des Kosten-Sicherheits-Verhältnisses der Teilnehmer zu betrachten. Am kostengünstigsten für den Teilnehmer ist der Einsatz eines Softwarezertifikates, das auf seiner Festplatte oder, schon sicherer, auf einer

Diskette gespeichert ist. Das damit erreichte Sicherheitsniveau ist jedoch als zu gering für Klasse niedrig einzustufen, da der Rechner der Teilnehmer nicht sicher genug gegenüber Viren und Trojaner eingeschätzt werden kann. Der Einsatz einer Chipkarte als Trägermedium des Zertifikates führt zu einer deutlichen Erhöhung des Sicherheitsniveaus, weil ein Angreifer in den Besitz der Chipkarte gelangen muß, um Mißbrauch vorzunehmen. Daher wird dieses Sicherheitsniveau für die Klasse niedrig ausgewählt. Um eine Chipkarte einsetzen zu können, muß der Teilnehmer jedoch zusätzliche Hardware in Form eines Chipkartenlesers erwerben. Hier könnten sich USB-Tokens[574] als Alternative anbieten, wenn die Kosten unterhalb einer Chipkarte samt Kartenleser liegen und vergleichbare Sicherheit vorliegt. Das höchste Sicherheitsniveau erreicht ein Teilnehmer mit einem signaturgesetzkonformen Chipkartenleser. Sämtliche genannten Klassen der Teilnehmer verfügen über eine ähnliches Kosten-Sicherheits-Verhältnis. Dieser Sachverhalt wird durch Abbildung 6-8 verdeutlicht.

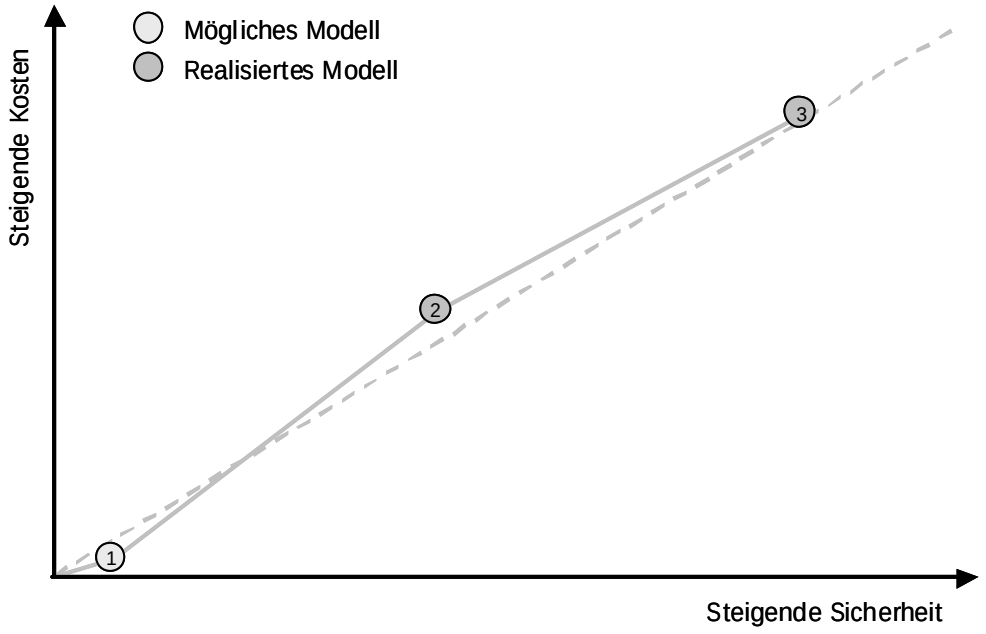

Abbildung 6-8 - Modelle des Teilaspekts Teilnehmer

[574] Für nähere Informationen vgl. Rainbow (iKey 2000, 2001), Internet-Quelle.

6.3 Auswahl der Sicherheitsstufen

In diesem Abschnitt werden Sicherheitsstufen für Zertifikate beziehungsweise Zertifizierungsstellen ausgewählt. In Kapitel 4.5 wurde der möglich Einsatz von Zertifikaten untersucht und festgestellt, daß die benötigte Sicherheit eines Zertifikates sehr eng mit dem Transaktionswert aus Sicht des Teilnehmers verknüpft ist. Dies hat zur Folge, daß aus Benutzersicht viele Stufen wünschenswert wären, um den jeweiligen Transaktionswert mit einem Zertifikat der korrespondierenden Sicherheitsstufe zu sichern. Dem entgegen wirkt jedoch die Tatsache, daß mit wachsender Anzahl der Sicherheitsstufen der Administrationsaufwand, nicht nur für die Teilnehmer, steigt. Als Ergebnis von Kapitel 4.5.3 ergaben sich zwei zu realisierende Stufen, mit einem niedrigen und einem hohen Sicherheitsniveau. Unabhängig von diesen Überlegungen wurden im vorherigen Abschnitt sämtliche Teilaspekte von Zertifizierungsstellen betrachtet und mögliche Modelle hinsichtlich ihres Sicherheitsniveaus und den entsprechenden Kosten bewertet.

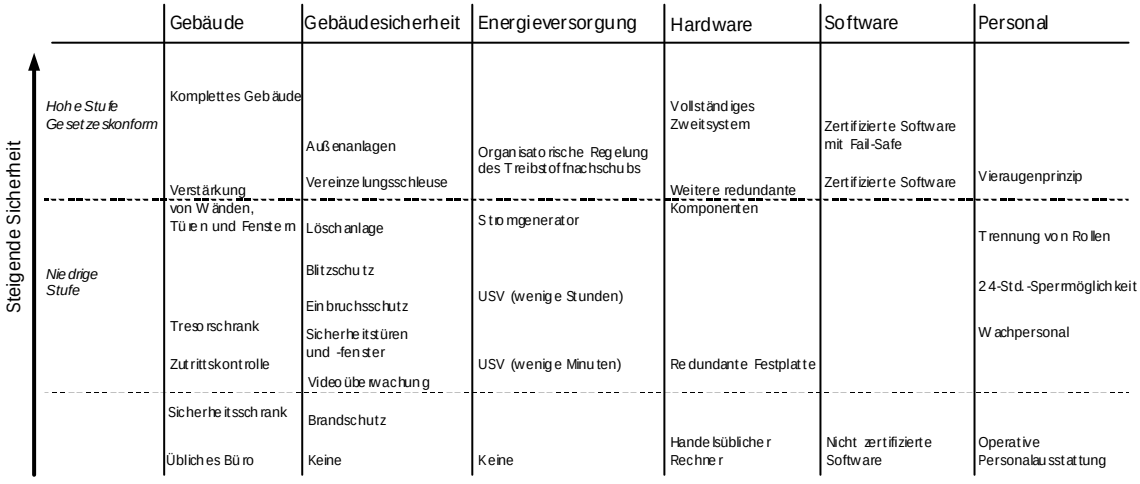

Abbildung 6-9 – Realisierte Sicherheitsstufen der unterschiedlichen Teilaspekte einer Zertifizierungsstelle

Nach Zusammenführung sämtlicher Teilaspekte, die Vorgehensweise ist detailliert in Kapitel 4.2.3 beschrieben, ergeben sich zwei Stufen von Zertifizierungsstellen, die im folgenden näher erläutert werden. Ausgehend von der Abbildung 5-2, die mögliche Sicherheitsstufen der unterschiedlichen Teilaspekte einer Zertifizierungs-

stelle darstellt, sind in Abbildung 6-9 die realisierten Sicherheitsstufen eingezeichnet. Zum einen eine niedrige Stufe, deren Zertifikate eine gewisse Sicherheit bieten und die deutlich von der Sicherheit des Verzichtes auf den Einsatz von Zertifikaten abzugrenzen ist. Zum anderen eine hohe Sicherheitsstufe, die den Vorgaben des Signaturgesetzes entspricht und damit Beweissicherheit für die eingesetzten Zertifikate bietet.

6.3.1 Niedrige Sicherheitsstufe

Für die niedrige Stufe werden die minimalen Maßnahmen zur Absicherung des Teilaspektes Gebäude angesetzt, was zur Folge hat, daß die komplette Zertifizierungsstelle innerhalb eines Raumes aufgebaut wird. Die Gebäudesicherheit kann sich damit auf den Schutz dieses Raumes beschränken. Die Energieversorgung stellt sicher, daß ein Stromausfall keinen Datenverlust zur Folge hat, für den tagelangen autarken Einsatz muß jedoch nicht vorgesorgt werden. Die Unterbringung des Verzeichnisdienstes auf einem getrennten Rechner in einem Rechenzentrum ist durch den damit verbundenen Schutz einer direkten Internetanbindung vorzuziehen. Zusätzlich zu den handelsüblichen Rechnern muß eine Software erworben werden, die den Betrieb der Zertifizierungsstelle ermöglicht. Selbst in der niedrigen Sicherheitsstufe sollten die Software ein Fail-Safe-Konzept beherrschen, da bereits mit der Kompromittierung eines Verfahrens die Infrastruktur zusammenbricht[575]. Der Einsatz eines Mitarbeiters und eventuell eines Vertreters im Krankheits- oder Urlaubsfall ist ausreichend, für die Sperrung von Zertifikaten sollte entweder eine Online-Lösung eingesetzt werden, die von Teilnehmern jederzeit verwendet werden kann. Dadurch wird die mißbräuchliche Sperrung von Zertifikaten zwar erleichtert, der daraus resultierenden mögliche Schaden sollte sich jedoch im wesentlich auf die Neuausstellung eines Zertifikates beschränken. Von den Teilnehmern muß der Einsatz eines Chipkarten-Lesegerätes erwartet werden, wobei die Eingabe der Legitimation durchaus per Software vonstatten gehen kann. Vom Einsatz einer reinen Softwarelösung ist abzuraten, da der heimische Rechner

[575] Vgl. Kapitel 4.4.4.

nicht als sicher gelten kann, wie die rasche Verbreitung von E-Mail-Viren und –Würmern zeigt[576]. Der Einsatz dieser Sicherheitsstufe als Mitarbeiter- oder Studentenausweis bringt darüber hinaus den Vorteil, daß die Zertifikatsausgabe vereinfacht werden kann, da die Daten bereits vorhanden sind und nicht erhoben und eingetragen werden müssen.

Die geschilderte Lösung ist für die Teilnehmer mit geringen Kosten verbunden, so daß der Besitz eines solchen Zertifikates für den Teilnehmer einen positiven Nutzen bringen kann. Für einen Einsatz bei jeglichen Transaktionen spricht für den Teilnehmer die erhöhte Sicherheit, selbst wenn ein Gericht letztlich die Beweisbarkeit der Transaktion durch ein solches Zertifikat negativ beurteilt. Das Risiko des Geschäftspartners, eine Transaktion trotz Zertifikates anzuzweifeln, erhöht sich auf jeden Fall beträchtlich, so daß eine Hemmschwelle entstehen wird[577].

6.3.2 Hohe Sicherheitsstufe – Signaturgesetzkonform

Soll eine hohe Stufe an Sicherheit erreicht werden, so müssen an das Gebäude besondere Anforderungen gestellt werden. Nach den Überlegungen im vorherigen Kapitel bleibt nur die Umsetzung der beschriebenen maximalen Stufe. Gleiches trifft für die Gebäudesicherung und die Energieversorgung zu. Ist eine Zertifikatssperrung aufgrund eines Stromausfalls nicht möglich, so wird der Schaden in dieser Sicherheitsstufe der Zertifizierungsstelle anzulasten sein, so daß die Notstromversorgung auf jeden Fall für mehrere Tage ausreichen muß. Eine Verlängerung dieser Überbrückungszeit ist durch organisatorische Maßnahmen sicherzustellen[578]. Heutige Rechenzentren entsprechen den Anforderungen des Gesetzgebers hinsichtlich des Gebäudes, der Gebäudesicherheit und der Energieversorgung, so daß der Verzeichnisdienst ausgelagert werden könnte[579]. Ungeachtet dieser Tatsache muß

---

[576] Vgl. Schmidt (Virenbasteln für Dummies, 2001), S. 98.

[577] Außerdem könnte, ähnlich der Faxnutzung, der durch die Nutzung entstehende Gewinn den Verlust durch fingierte Bestellungen mehr als ausgleichen.
Vgl. Wobst (Abenteuer Kryptologie, 1998), S. 357.

[578] Vgl. Stumm/Weber (Infrastruktur für Zertifizierungsstellen, 2000), S. 6.

[579] Vgl. Tiscali (Tiscali.host, 2001), S. 3.

der Verzeichnisdienst samt der Online-Abfrage des Zertifikatsstatus redundant unter verschiedenen IP-Adressen erreichbar sein, so daß im Falle eines DDoS-Angriffs die Verfügbarkeit gewährleistet ist. Gerade durch die Einfachheit der Durchführung eines solchen Angriffs, im Gegensatz zur Durchführung eines physischen Angriffs auf das Gebäude der Zertifizierungsstelle oder ein Rechenzentrum, ist dieser Angriff am wahrscheinlichsten. Wie weiter oben beschrieben, ist die Sicherheit der Software unproblematisch und muß in dieser Sicherheitsstufe durch Zertifizierungen nachgewiesen werden. Zusätzlich muß ein Fail-Safe-Konzept vorliegen, obwohl dies oftmals vergessen oder gar ignoriert wird[580]. Trotz der hohen Kosten des Personals im Verhältnis zu den anderen Teilaspekten einer Zertifizierungsstelle[581], muß ein hohes Sicherheitsniveau entsprechend umgesetzt werden. Ein Teilnehmer muß der hohen Sicherheitsstufe durch den Einsatz signaturgesetzkonformer Chipkarten-Lesegeräte Rechnung tragen, die über eine Eingabemöglichkeit der Authorisierungs-PIN verfügen.

Nicht nur dadurch sind die Kosten für einen Teilnehmers dieser Sicherheitsstufe als hoch anzusehen und der Zeitaufwand um ein Zertifikat zu erhalten entsprechend. Um diese Kosten durch genügenden Nutzen kompensieren zu können, müßten entsprechend viele Transaktionen mit hohem Wert für den Teilnehmer möglich sein, was zum gegenwärtigen Zeitpunkt nicht der Fall ist. Unternehmen bietet sich damit die Möglichkeit, B2B-Transaktionen entsprechend abzusichern, jedoch werden die Teilnehmerzahlen der Mitarbeiter von Unternehmen ebenfalls gering bleiben, weil nicht jeder Mitarbeiter ein Zertifikat dieser Sicherheitsstufe benötigt.

6.4 Ergebnis

Als wichtigstes Ergebnis der vorangegangenen Betrachtungen läßt sich festhalten, daß die Einführung signaturgesetzkonformer Zertifizierungsstellen wirtschaftlich

---

[580] Vgl. Langenbach/Ulrich (Elektronische Signaturen, 2002), S. 100.

[581] Vgl. Kapitel 5.2.1, insbesondere Kapitel 5.2.1.2.

nicht möglich ist, ohne daß vorher die entsprechende Basis an Teilnehmerakzeptanz[582] durch implementierte Vorgänge niedriger Sicherheit erreicht worden ist[583]. Da der Teilnehmer durch das Verbraucherschutzgesetz über ausreichenden Schutz verfügt, besteht überhaupt keine Notwendigkeit, die Transaktionen zusätzlich durch den Einsatz von Zertifikaten zu sichern. Bei der verschlüsselten Übertragung der Kreditkartendaten kann ein Online-Käufer auf die Sicherheit von SSL oder auf die der Kreditkartenbestimmungen vertrauen[584].

Damit sich die PKI-Technologie durchsetzen kann, müssen Basisanwendungen mit großer Verbreitung umgesetzt werden. Als wichtigste Anwendungsmöglichkeiten sind in diesem Zusammenhang Authentifikation und Single-Sign-On zu nennen[585]. Diese können von Unternehmen mit Hilfe einer eigenen Zertifizierungsstelle kostengünstig eingeführt werden. Gleiches gilt für Universitäten, die durch die Einführung digitaler Studienausweise häufige Prozesse, als wichtigster sei die Erstellung eines Leistungsnachweises genannt, elektronisch abbilden und damit Kosten sparen können. In beiden genannten Fällen werden sämtliche Kosten der Rechnungsstellung gespart, da Unternehmen die Ausweise kostenlos an Mitarbeiter verteilen und Universitäten diese Kosten im Zuge der Studiengebühren einziehen können.

Dies ist insbesondere wichtig, weil die Teilnehmer gezwungen würden, mit den Chipkarten umzugehen. Sie würden mit der Problematik vertraut gemacht, daß Sicherheit zu Lasten der Benutzerfreundlichkeit und des Komforts geht[586]. Jeder Teilnehmer muß damit für sich selbst entscheiden, wieviel Wert der Sicherheit beigemessen wird.

Im nächsten Schritt sollten sich einzelne Unternehmen cross-zertifizieren, so daß die Mitarbeiter beider Unternehmen bei der Kommunikation auf Zertifikate zu-

---

[582] Vgl. Böhmer (Erfahrungen beim Einsatz und Aufbau einer PKI, 2001), S. 451.

[583] Vgl. Fox (E-Mail-Sicherheit, 2001), S. 453;
Vgl. Böhmer (Erfahrungen beim Einsatz und Aufbau einer PKI, 2001), S. 447.

[584] Vgl. Schneier (Secrets & Lies, 2001), S. 232.

[585] Vgl. Paulus (Rundum-sorglos Paket mit Hindernissen, 2001), S. 529.

[586] Vgl. Russell/Cunningham (Maximum Protection, 2001), S. 216.

rückgreifen und diese verwenden könnten. Insbesondere bei Unternehmen der Zulieferindustrie, die häufig mit wenigen Unternehmen kommunizieren, ist dies zu empfehlen. Als Erweiterung sollten im nächsten Schritt Unternehmen Bridge-Dienste anbieten und als Brückenzertifizierungsstelle am Markt auftreten, und so beliebige Unternehmen oder öffentliche Einrichtungen über eine genormte Schnittstelle verbinden[587]. Auf diesem Wege könnten sich Zertifikate sukzessive verbreiten bis Netzwerkeffekte die Verbreitung der Zertifikates unterstützen[588].

Verschiedene Bridges sollten im nächsten Schritt konkurrieren, um eine Monopolsituation zu vermeiden. An dieser Stelle bleibt es dem Markt überlassen, ob einzelne Bridges über die minimal nötige Sicherheit hinaus aktiv werden und mit zusätzlicher Sicherheit werben. Als Voraussetzung zur Teilnahme könnten Sicherheitsauflagen gesetzt werden, so daß die Bridges eine neue Klasse der Sicherheit einführen würden.

Im letzten Schritt würden Bridges mit der Sicherheitsauflage des Signaturgesetzes notwendig, wie dies heute schon von der RegTP angeboten wird[589]. Damit hätten alle dort angeschlossenen Zertifizierungsstellen beweisbar sichere Zertifikate. Mit der damit einhergehenden Steigerungsrate an Teilnehmern würde genügend Nachfrage geschaffen, weitere Prozesse, besonders mit hohem Sicherheitsniveau, elektronisch abzubilden und online verfügbar zu machen.

---

[587] Vgl. Reif (Bridge-CA, 2001), S. 553.

[588] Vgl. Zerdick (Die Internet-Ökonomie, 2001), S. 214ff.

[589] Eine Brückenzertifizierungsstelle entspricht einer zweistufigen Hierarchie, bei der die Zertifikate nicht durch die Wurzelzertifizierungsstelle ausgegeben werden, sondern statt dessen cross-zertifiziert. Genauer Erläuterungen finden sich in Kapitel 4.1.2.

7 Schlußbetrachtung

Nachdem die Teilnehmerzahlen für digitale Signaturen deutlich hinter den Erwartungen zurückbleiben, stellt sich die Frage nach den Gründen. Aus diesem Grund hat die vorliegende Arbeit zwei Zielsetzungen verfolgt, die eng miteinander verknüpft sind. Das eine Ziel bestand darin zu überprüfen, ob ein wirtschaftlicher Betrieb einer Zertifizierungsstelle mit hohem Sicherheitsniveau, das heißt beweisbar sicheren Zertifikaten, möglich ist. Es wurde gezeigt, daß dies nach der herrschenden Gesetzeslage und den vorhandenen Nutzungsmöglichkeiten nicht möglich sein kann[590]. Das andere Ziel beinhaltete die Untersuchung, inwiefern der Betrieb von Zertifizierungsstellen eines niedrigen Sicherheitsniveaus wirtschaftlich sein kann. Dies bedeutet, daß der aus dem Einsatz eines Zertifikates entstehende Nutzen des Teilnehmers seine Kosten übersteigt. Dazu wurden die notwendigen Voraussetzungen erläutert und ein allgemeines Verfahren entwickelt, das die Bewertung des erreichten Sicherheitsniveaus mit Blick auf die damit zusammenhängenden Kosten ermöglichte. In Verbindung mit den dargestellten Alternativen im Bereich der Rahmenbedingungen für Zertifizierungsstellen wurde ein Weg erarbeitet, der langfristig den wirtschaftlichen Betrieb von Zertifizierungsstellen mit einem hohen Sicherheitsniveau ermöglichen könnte.

Im zweiten Kapitel wurden die benötigten technischen Grundlagen erläutert, die die Basis für den Einsatz digitaler Signaturen bilden. Nach den Anforderungen an die elektronische Kommunikation wurden kryptographische Grundlagen beschrieben, die zur Erstellung einer digitalen Signatur benötigt werden und eine Ein-

---

[590] Mittlerweile hat sich mit der Deutschen Post-Tochter Signtrust ein großer Anbieter von digitalen Signaturen aus dem Geschäft zurückgezogen.

Vgl. Wilkens (Deutsche Post ohne Online-Geschäft, 2002), S. 43;

Vgl. o.V. (Markt noch nicht reif, 2002), S. 1.

schätzung des damit verbundenen Risikos ermöglichen. Im Anschluß daran wurde im Abschnitt Protokolle aufgezeigt, daß der Einsatz kryptographischer Erweiterungen von vorhandenen Protokollen und kryptographischer Protokolle ausreicht, um die geschilderten Anforderungen an die elektronische Kommunikation zu erfüllen. Als Verbindung von öffentlichen Schlüsseln zu realen Identitäten und damit als Möglichkeit des Austausches öffentlicher Schlüssel über unsichere Netze wurden Zertifikaten, hinsichtlich Ihres Aufbaus und Einsatzes, vorgestellt. Des weiteren wurden die Wiederherstellung von Schlüsseln und der Einsatz von Mitarbeiterzertifikaten diskutiert. Zum Abschluß der technischen Grundlagen wurden Zertifizierungsstellen als vertrauenswürdige Dritte vorgestellt und auf die Eigenschaften von Zertifikatsketten beim Einsatz von Zertifikaten eingegangen. Dies stellte die Vorbedingung für die im vierten Kapitel erläuterten Vertrauensverfahren dar.
Im Anschluß an die technischen Grundlagen wurden im dritten Kapitel die rechtlichen Grundlagen für Zertifizierungsstellen beschrieben, wobei dieses Kapitel wiederum in zwei Abschnitte aufgeteilt war. Im ersten Abschnitt wurden die Gesetze vorgestellt, die Auswirkungen auf den Aufbau von Zertifizierungsstellen ausüben, angefangen bei der europäischen Signaturrichtlinie über das deutsche Signaturgesetz und die Signaturverordnung bis zum IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik. Aus der deskriptiven Beschreibung wurde deutlich, daß ihnen keine Anleitung zum Bau einer Zertifizierungsstelle zu entnehmen ist. Daher wurden im zweiten Abschnitt die Auswirkungen der Gesetze auf die Funktionalität und die Infrastruktur einer signaturgesetzkonformen Zertifizierungsstelle geschildert, die in der Kostenbetrachtung Berücksichtigung fanden.
Im vierten Kapitel wurden Rahmenbedingungen für Zertifizierungsstellen betrachtet. Aufbauend auf der Beschreibung von Zertifikatsketten im zweiten Kapitel, wurden im ersten Abschnitt Vertrauensverfahren für Zertifizierungsstellen erörtert. Aus diesem Grund wurden ausgehend von Vertrauensverfahren für Personen alternative Verfahren für Zertifizierungsstellen vorgestellt. Bei diesem Vergleich wurde der Vorteil eines Einsatzes von Brückenzertifizierungsstellen gegenüber der im Signaturgesetz vorgeschriebenen zweistufigen Hierarchie deutlich. Im zweiten

Abschnitt des Kapitels wurden Klassifizierungskriterien für Zertifikate untersucht. Ausgehend von der gegebenen Unterteilung in beweisbar sicher oder nicht wurde eine Einteilung nach der Formbedürftigkeit der Transaktion oder nach der Beweiskraft der Zertifikate aus der Literatur diskutiert. Den Kern des Abschnitts bildete jedoch die neu entwickelte Klassifizierung nach dem Kosten-Sicherheits-Verhältnis, bei dem eine mögliche Einteilung direkt aus den denkbaren Zertifizierungsstellen anhand der zugrundeliegenden Kosten und des erreichten Sicherheitsniveaus ermittelt wird. Dieser neue Ansatz betrachtet erstmals nicht nur das Sicherheitsniveau, sondern erlaubt durch die Verknüpfung mit den Kosten eine Bewertung, ob zwei verschiedene Sicherheitsniveaus wirtschaftlich sinnvoll zu implementieren sind, oder ob eine Zusammenlegung nicht vorteilhafter wäre. Im dritten Abschnitt fand eine Darstellung der Prozesse einer Zertifizierungsstelle statt, die den Teilnehmern in Rechnung gestellt werden können. Dabei wurde berücksichtigt, ob ein Prozeß aus wirtschaftlicher Sicht alleine oder besser in Verbindung mit anderen Prozessen angeboten werden sollte. Aufbauend auf den kryptographischen Grundlagen des zweiten Kapitels wurden im vierten Abschnitt Angriffsmöglichkeiten gegen Zertifikate oder mathematische Verfahren beschrieben, um die Wahrscheinlichkeit eines Angriffs bewerten zu können. Den Abschluß des Kapitels bildete eine Bedarfsanalyse, die den Markt für Zertifikate geeignet segmentierte und eine Schätzung der Menge benötigter Zertifikate der unterschiedlichen Sicherheitsniveaus lieferte. Die sich ergebenden notwendigen Sicherheitsniveaus beeinflußten die Einteilung in Sicherheitsstufen im sechsten Kapitel.

Im fünften Kapitel wurde nach einer kurzen Einführung in die verwendete Kostenrechnung eine Betrachtung der Wirtschaftlichkeit einer Zertifizierungsstelle durchgeführt, die im wesentlichen auf einer Kostenbetrachtung von Zertifizierungsstellen unterschiedlicher Sicherheitsniveaus beruhte. Als Vorgehensweise bei der Bestimmung der Kosten wurde die Zertifizierungsstelle nach den in Kapitel drei erläuterten Infrastrukturkomponenten zerlegt und jeweils sukzessive von minimal nötigen bis durch das Signaturgesetz vorgeschriebenen und damit maximalen Maßnahmen zur Erhöhung der Sicherheit aufgebaut und monetär bewertet. Insbesondere die Bewertung der Sicherheit einzelner Maßnahmen orientierte sich

an den im vierten Kapitel beschriebenen Angriffen gegen Zertifizierungsstellen beziehungsweise die angebotenen Zertifikate. Die Summe sämtlicher Kosten der Infrastruktur zuzüglich der Personal- und Materialkosten ergab die Gesamtkosten einer Zertifizierungsstelle. Um die Wirtschaftlichkeit ermitteln zu können, wurden die fixen und variablen Kosten bestimmt und auf ein Zertifikat umgelegt. Mit der Einbeziehung der fixen Kosten konnten für verschiedene Szenarien an Teilnehmern, und damit verkauften Zertifikaten, die Kosten eines Zertifikates einer Zertifizierungsstelle errechnet werden. Zusammen mit der Bedarfsanalyse aus dem vorherigen Kapitel und den empirisch ermittelten Marktpreisen eines signaturgesetzkonformen Zertifikates konnte die Wirtschaftlichkeit einer Zertifizierungsstelle eingeschätzt werden. Im Ergebnis mußte festgestellt werden, daß der wirtschaftliche Betrieb von Zertifizierungsstellen nach dem Signaturgesetz, und damit beweisbar sicheren Zertifikaten, nicht möglich ist. Damit war das erste Ziel der Arbeit erreicht. Nachdem die Voraussetzungen zur Erreichung des zweiten Ziels insbesondere durch die Entwicklung des Kosten-Sicherheits-Verfahrens zur Bewertung der Wirtschaftlichkeit gegeben waren, mußte dieses Verfahren im folgenden nur noch zur Anwendung kommen.

Aus diesem Grund wurden im sechsten Kapitel unabhängig von dem bei der vorhergehenden Analyse erzielten Ergebnis Sicherheitsstufen für Zertifizierungsstellen gebildet, die neben der signaturgesetzkonformen Stufe mit beweisbar sicheren Zertifikaten einen wirtschaftlichen Betrieb ermöglichen könnten. Grundlage der Durchführung bilden die im fünften Kapitel ermittelten Kosten, die bei der sukzessiven Erhöhung der Sicherheit einzelner Infrastrukturkomponenten anfallen. Mit Hilfe dieser Daten konnten im dritten Abschnitt zwei Sicherheitsstufen beschrieben werden, die ein niedriges und ein hohes Sicherheitsniveau darstellen. Die tatsächlich anfallenden Kosten sind an dieser Stelle nicht gesondert zu betrachten, da diese durch die Anwendung des Kosten-Sicherheits-Verhältnisses implizit berücksichtigt sind. Die erhaltenen Stufen bilden jede für sich eine kostenoptimale Implementierung des gewünschten Sicherheitsniveaus. Zum Abschluß des Kapitels wurde daher unter Berücksichtigung der Rahmenbedingungen für Zertifizierungsstellen des vierten Kapitels ein Weg skizziert, der den wirtschaftlichen Betrieb

von Zertifizierungsstelle der niedrigen und langfristig den der hohen Sicherheitsstufe mit beweisbar sicheren Zertifikaten ermöglichen könnte. Die Erfüllbarkeit der den zeitlichen Horizont dieser Entwicklung determinieren Vorraussetzungen wurde ebenfalls gezeigt. Nach einer gesellschaftlichen Neueinschätzung des Vorgehens bei der Einführung von digitalen Signaturen steht aus diesem Grund einer erfolgreichen Nutzung nichts mehr im Wege. Gerade im Hinblick auf die möglichen Einsparpotentiale durch die weitere Automatisierung von Vorgängen und Fortschritte im Bereich des elektronischen Handels ist dies ein Ergebnis, das der digitalen Signatur die Einschätzung zukunftsfähig unter geänderten Voraussetzungen erhält.

Literaturverzeichnis

Adams, C. / Lloyd, S. (Understanding Public-Key-Infrastructure, 1999):
Understanding Public-Key-Infrastructure: Concepts, Standards, and Deployment Considerations, Indianapolis 1999.

Alpar, P. (Kommerzielle Nutzung des Internet, 1998):
Kommerzielle Nutzung des Internet, 2. Aufl., Berlin 1998.

Altmann, P. (Federal Bridge Certification Authority, 2001):
The US Federal PKI and the Federal Bridge Certification Authority, in: Computer Networks, 37, S. 685-690.

American National Standards Institute (ASCII, 1997):
ANSI X3.4-1986 (R1997) American National Standard Code for Information Interchange (ASCII), Online im Internet unter URL: http://www.ansi.org - Dokument: ANSI INCITS 4-1986 (R1997) (27.12.2001).

Anderson, R. / Diffie, W. / Neumann, P. G. / Rivest, R. L. / Schneier, B. and more (The risks of key recovery, 2001):
The risks of key recovery, key escrow & trusted third party encryption, Online im Internet unter URL: http://www.cdt.org/crypto/risks98/ (27.12.2001).

ARD-Ratgeber Recht Vieraugenprinzip (Vieraugenprinzip, 2001):
Rechtswörterbuch Vieraugenprinzip, Online im Internet unter URL: http://www.wdr.de/tv/recht/worte/rw04188.html (27.12.2001).

Aster, M. v. (Neuropsychologische Testbatterie für Zahlenverarbeitung, 2001):
Neuropsychologische Testbatterie für Zahlenverarbeitung und Rechnen bei Kindern, Frankfurt/Main 2001.

Bager, J. (Microsoft warnt vor Cracker-Zertifikat, 2001):
Microsoft warnt vor Cracker-Zertifikat, Online im Internet unter URL:
http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/jo-24.03.01-001/default.shtml&words=Microsoft%20Zertifikat (13.08.2002).

Barber, R. (Implementing Public Key Infrastructures, 2000):
Implementing Public Key Infrastructures in a Dynamic Business Environment, in: Computer & Security, No. 3, S. 230-233.

Baum, M. (Gültigkeitsmodell des SigG, 1999):
Gültigkeitsmodell des SigG, in: Datenschutz und Datensicherheit, 4/1999, S. 199-205.

Bea, F. X. / Dichtl, E. / Schweitzer, M. (Allgemeine Betriebswirtschaftslehre Bd. 1: Grundfragen, 2000):
Allgemeine Betriebswirtschaftslehre Bd. 1: Grundfragen, 8. Aufl., Stuttgart 2000.

Bea, F. X., / Dichtl, E. / Schweitzer, M. (Allgemeine Betriebswirtschaftslehre Bd. 2: Führung, 2001):
Allgemeine Betriebswirtschaftslehre Bd. 2: Führung, 7. Aufl., Stuttgart 2001.

Becker, T. / Dusemund, B. / Gollan, L. / Engel, T. / Meinel, C. (Infrastructure, Specifications and Standards, 2000):
Trust Centre: Infrastructure, Specifications and Standards, Online im Internet unter URL: http://www.ti.fhg.de/publikationen/studien_und_bucher/index.html (27.12.2001).

Belke, M. (Die Digitale Signatur kurz vor dem Start, 2000):
Die Digitale Signatur kurz vor dem Start - Perspektive SigG-konformer Trustcenter, in: Datenschutz und Datensicherheit, 2/2000, S. 74-76.

Berger, A. (Signatur-Interoperabilitätsspezifikation, 1998):
Signatur-Interoperabilitätsspezifikation: Zertifikaten und Dokumente, in: Datenschutz und Datensicherheit, 4/1998, S. 206-212.

Berners-Lee, T. / Connolly, D. (HTML - RFC 1866, 1995):
Hypertext Markup Language 2.0 (HTML) - RFC 1866, Online im Internet unter URL: http://www.ietf.org/rfc/rfc1866.txt?number=1866 (27.12.2001).

Berners-Lee, T. / Fielding, R. / Frystyk, H. (HTTP/1.0 - RFC 1945, 1996):
Hypertext Transfer Protocol (HTTP/1.0) - RFC 1945, Online im Internet unter URL: http://www.ietf.org/rfc/rfc1945.txt?number=1945 (27.12.2001).

Bernstein, D. J. (Internet mail message header format, 2001):

Internet mail message header format, Online im Internet unter URL: http://cr.yp.to/immhf.html (27.12.2001).

Bertsch, A. (Digitale Signaturen, 2001):

Digitale Signaturen, Berlin 2001.

Bertsch, A. / Pordesch, U. (Problematik von Prozeßlaufzeiten, 1999):

Zur Problematik von Prozeßlaufzeiten bei Sperrung von Zertifikaten, in: Datenschutz und Datensicherheit, 9/1999, S. 514-519.

Betge, P. (Investitionsplanung, 1998):

Investitionsplanung: Methoden - Modelle - Anwendungen, 3. Aufl., Wiesbaden 1998.

Biham, E. / Shamir, A. (Differential cryptanalysis, 1991):

Differential cryptanalysis of DES-like cryptosystems, in: Advances in Cryptology Crypto, 1991, S. 2-21.

Bitzer, F. / Brisch, K. M. (Digitale Signatur, 1999):

Digitale Signatur, Berlin 1999.

Blum, F. (Entwurf eines neuen Signaturgesetzes, 2001):

Entwurf eines neuen Signaturgesetzes, in: Datenschutz und Datensicherheit, 2/2001, S. 71-78.

BMWi / BMI / BSI (Haushaltswirtschaftssystem auf Basis digitaler Signaturen, 2001):

Haushaltswirtschaftssystem auf Basis digitaler Signaturen, Online im Internet unter URL: http://www.sicherheit-im-internet.de/themes/print.phtml?ttid=38&tdid=1140 (27.12.2001).

Böhmer, I. (Erfahrungen beim Einsatz und Aufbau einer PKI, 2001):

Erfahrungen beim Einsatz und Aufbau einer konzernweiten PKI, in: Datenschutz und Datensicherheit, 8/2001, S. 446-451.

Bohr, K. (Wirtschaftlichkeit, 1993):

Wirtschaftlichkeit, in: Chmielewicz, K. / Schweitzer, M. (Hrsg.), Enzyklopedie der Betriebswirtschaftslehre: Band 3. Handwörterbuch des Rechnungswesens, 3. Auflage, Stuttgart, 1993, Sp. 2181-2188.

Bonder, A. ("PKIs sind noch nicht alltagstauglich", 2001):

PKIs sind noch nicht alltagstauglich, in: Computerwoche, 23/2001, S. 24.

Born, A. (Ware Arbeit, wahrer Lohn, 2001):

Ware Arbeit, wahrer Lohn, Online im Internet unter URL: http://www.heise.de/ix/artikel/2001/07/114/ (27.12.2002).

Brazier, J. R. T. (Possible NSA Decryption Capabilities, 1999):

Possible NSA Decryption Capabilities, in: Datenschutz und Datensicherheit, 10/1999, S. 576-581.

Bressoud, D. M. (Factorization and primality testing, 1989):

Factorization and primality testing, New York 1989.

Brill, C.-W. (Elektronischer Stempel, 2001):

Basis - Sicherheitsinfrastruktur, Institutionskarte und elektronischer Stempel, in: Datenschutz und Datensicherheit, 9/2001, S. 546-548.

BSI (SigI, 1999):

Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV, Online im Internet unter URL: http://www.bsi.de/esig/basics/techbas/interop/bsi/index.htm (27.12.2001).

BSI (SigI - Zeitstempel, 1999):

Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV - A4 Zeitstempel, Online im Internet unter URL: http://www.bsi.de/esig/basics/techbas/interop/bsi/sigi-a4.pdf (27.12.2001).

BSI (Signatur-Interoperabilitätsspezifikation, 1999):

Spezifikation zur Entwicklung interoperabler Verfahren nach SigG / SigV Signatur-Interoperabilitätsspezifikation SigI, Online im Internet unter URL: http://www.bsi.bund.de/esig/basics/techbas/interop/bsi/sigi-a6.pdf (20.02.2002).

BSI (IT-Grundschutzhandbuch, 2001):

IT-Grundschutzhandbuch, Online im Internet unter URL: http://www.bsi.bund.de/gshb/deutsch/menue.htm (27.12.2001).

BSI (IT-Grundschutz-Zertifikat, 2001):

IT-Grundschutz-Zertifikat, Online im Internet unter URL: http://www.bsi.bund.de/gshb/zert/index.htm (27.12.2001).

BSI (ITSEC, 2001):

ITSEC, Online im Internet unter URL: http://www.bsi.de/zertifiz/itkrit/itsec-dt.pdf (27.12.2001).

BSI (Vergleich CC - ITSEC, 2001):

Vergleich CC - ITSEC, Online im Internet unter URL: http://www.bsi.bund.de/literat/faltbl/cc.htm#VergleichCC (27.12.2001).

Buchmann, J. (Faktorisierung großer Zahlen, 1999):

Faktorisierung großer Zahlen, in: Spektrum der Wissenschaft, Heft 2/1999, S. 6-13.

Buchmann, J. (Wie sicher kann Sicherheit sein, 2001):

Wie sicher kann Sicherheit sein, Online im Internet unter URL: http://www.informatik.tu-darmstadt.de/ftp/pub/TI/TR/TI-01-05.WieSicherKannSicherheitSein.ps.gz (27.12.2001).

Büllingen, F. / Hillebrand, A. / Stamm, P. (IT-Sicherheit als Standortfaktor, 2000):

IT-Sicherheit als Standortfaktor, in: Datenschutz und Datensicherheit, 10/2000, S. 598-602.

Bundesanzeiger (Geeignete Kryptoalgorithmen, 2000):

Geeignete Kryptoalgorithmen gemäß §17 (2) SigV, Online im Internet unter URL: http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/23.pdf (27.12.2001).

Bundesanzeiger (Nr. 158, 2001):

Nr. 158, Bonn 2001.

Bundesdruckerei GmbH (Personalausweis/Reisepaß, 2001):

Personalausweis/Reisepaß, Online im Internet unter URL: http://www.bundesdruckerei.de/de/produkte/2_1_3.html (27.12.2001).

Bundesministerium der Finanzen (AfA-Tabelle, 2000):

AfA-Tabelle für die allgemein verwendbaren Anlagegüter (AV), Online im Internet unter URL: http://www.bundesfinanzministerium.de/Anlage5066/AfA-Tabellen.zip (27.12.2001).

Camphausen, I. / Kelm, S. / Liedke, B. / Weber, L. (Aufbau und Betrieb einer Zertifizierungsinstanz, 2001):

Aufbau und Betrieb einer Zertifizierungsinstanz (DFN-PCA Handbuch), Online im Internet unter URL: http://www.cert.dfn.de/dfn/berichte/db089/ (27.12.2001).

Chadwick, D. W. / Basden, A. (Evaluation Trust in a Public Key Certification Authority, 2001):

Evaluation Trust in a Public Key Certification Authority, in: Computer & Security, 20 Nr. 7, S. 592-611.

Coenenberg, A. G. (Kostenrechnung und Kostenanalyse, 1999):

Kostenrechnung und Kostenanalyse, 4. Aufl., Landsberg/Lech 1999.

Common Criteria (Common Evaluation Methodology, 1999):

Common Evaluation Methodology der Common Criteria, Online im Internet unter URL: http://www.commoncriteria.org/docs/PDF/CEMV10.PDF (27.12.2001).

Crispin, M. (IMAP4 - RFC 1730, 1994):

Internet Message Access Protocol - Version 4 (IMAP4) - RFC 1730, Online im Internet unter URL: http://www.ietf.org/rfc/rfc1730.txt?number=1730 (14.07.2002).

Davidson, G. C. / Neale, J. M. (Klinische Psychologie, 1998):

Klinische Psychologie, 5. Aufl., Weinheim 1998.

Deutsche Bank AG/Deutsche Telekom AG (Bridge-CA, 2001):

Bridge-CA, Online im Internet unter URL: http://www.bridge-ca.org/ (12.12.2001).

Deutsche Post (Post Ident 3, 2001):

Post Ident 3 - Eine sichere Basis für Ihre Kundenkontakte, Online im Internet unter URL: http://www.deutschepost.de/brief/produkte-services/postident/p3_beschreibung.html (27.12.2001).

Deutsche Telekom AG (Public Key Service Informationen, 2001):

Public Key Service Informationen, Online im Internet unter URL: http://www.dtag.de/dtag/t-telesec/telesec_showdatei/1,2626,14,00.pdf (27.12.2001).

Deutsche Telekom AG (Servicerufnummern, 2002):

Servicerufnummern - Bei Anruf Service, Online im Internet unter URL: http://www.telekom.de/dtag/ipl2/cda/mr2/0,15187,20129110000 1445,00.html (21.07.2002).

Diedrich, O. (Preiswerte Hochleistungsrechner mit Clustern, 2000):

Einigkeit macht stark - Preiswerte Hochleistungsrechner mit Clustern, in: c't, Heft 22, S. 234-239.

Diffie, W. / Hellmann, M. E. (New Directions in Cryptography, 1976):

New Directions in Cryptography, in: IEEE Transactions on Information Theory, IT-22 (6), S. 644-654.

Dittmann, J. (Digitale Wasserzeichen, 2001):

Digitale Wasserzeichen, Berlin 2001.

Dobbertin, H. / Bosselaers, A. / Preneel, B. (The hash function RIPEMD-160, 2001):

The hash function RIPEMD-160, Online im Internet unter URL: http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html (27.12.2001).

Domschke, W. / Drexl, A. (Einführung in Operations Research, 1995):

Einführung in Operations Research, 3. Aufl., Berlin 1995.

Domschke, W. / Scholl, A. (Grundlagen der Betriebswirtschaftslehre, 2002):
Grundlagen der Betriebswirtschaftslehre - Eine Einführung aus entscheidungsorientierter Sicht, 2. Aufl., Berlin 2002.

Dusemund, B. / Becker, T. / Gollan, L. / Engel, T. / Meinel, C. (The Functionality of a Public Key Infrastructure, 2000):
Security in Open Networks: The Functionality of a Public Key Infrastructure, Online im Internet unter URL: http://www.ti.fhg.de/publikationen/technische_berichte/2000/prep1500.pdf (27.12.2001).

Eastlake, D. / Jones, P. (SHA1 - RFC 3174, 2001):
US Secure Hash Algorithm 1 (SHA1) - RFC 3174, Online im Internet unter URL: http://www.ietf.org/rfc/rfc3174.txt?number=3174 (27.12.2001).

Eckert, C. (IT-Sicherheit, 2001):
IT-Sicherheit, München 2001.

Esslinger, B. / Barcklow, D. / Bartosch, M. (Global PKI and S/MIME Interoperability, 2001):
Global PKI and S/MIME Interoperability - The European Bridge-CA Initative, in: Datenschutz und Datensicherheit, 9/2001, S. 519-525.

Falk, R. / Trommer, M. (Nutzung von Verzeichnisdiensten, 1999):
Nutzung von Verzeichnisdiensten zur integrierten Verwaltung heterogener Sicherheitsmechanismen, in: Sicherheitsinfratrukturen, in Horster, P. (Hrsg), S. 96-108.

Federrath, H. / Pfitzmann, A. (Schutzziele in IT-Systemen, 2000):
Gliederung und Systematisierung von Schutzzielen in IT-Systemen, in: Datenschutz und Datensicherheit, 12/2000, S. 704-710.

Feess-Dörr, E. (Microökonomie, 1995):
Microökonomie: eine Einführung in die neoklassische und klassische neoricadianische Preis- und Verteilungstheorie, Marburg 1995.

Feghhi, J. / Feghhi, J. / Williams, P. (Digital Certificates, 1999):
Digital Certificates - Applied Internet Security, Reading 1999.

Fell, H.-W. (Interoperabilität in PKI-Anwendungen, 2001):
Interoperabilität in PKI-Anwendungen - Notwendigkeit oder Marketingfloskel, in: Datenschutz und Datensicherheit, 9/2001, S. 536-538.

Fielding, R. / Gettys, J. / Frystyk, H. / Berners-Lee, T. (HTTP/1.1 - RFC 2068, 1997):
Hypertext Transfer Protocol (HTTP/1.1) - RFC 2068, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2068.txt?number=2068 (27.12.2001).

Fielding, R. / Gettys, J. / Mogul, J. / Frystyk, H. / Masinter, L. / Leach, P. / Berners-Lee, T. (HTTP/1.1 - RFC 2616, 1999):
Hypertext Transfer Protocol (HTTP/1.1) - RFC 2616, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2616.txt?number=2616 (27.12.2001).

Ford, W. / Baum, M. S. (Secure Electronic Commerce, 1997):
Secure Electronic Commerce, New Jersey 1997.

Fox, D. (Certification Practice Statement, 1999):
Certification Practice Statement, in: Datenschutz und Datensicherheit, 4/1999, S. 230.

Fox, D. (Die Regulierung der Nullmenge, 1999):
Die Regulierung der Nullmenge, in: Datenschutz und Datensicherheit, 9/1999, S. 494.

Fox, D. (Eine kritische Würdigung des SigG, 1999):
Eine kritische Würdigung des SigG, in: Datenschutz und Datensicherheit, 9/1999, S. 508-510.

Fox, D. (Certification Revocation List (CRL), 2001):
Certification Revocation List (CRL), in: Datenschutz und Datensicherheit, 8/2001, S. 485.

Fox, D. (Cross-Zertifikat, 2001):
Cross-Zertifikat, in: Datenschutz und Datensicherheit, 3/2001, S. 105.

Fox, D. (E-Mail-Sicherheit, 2001):
E-Mail-Sicherheit, in: Datenschutz und Datensicherheit, 8/2001, S. 452-458.

Fox, D. (Misserfolgsbegeisterung, 2001):
Misserfolgsbegeisterung, in: Datenschutz und Datensicherheit, 6/2001, S. 314.

Fox, D. (Preis der Pioniertat, 2001):

Preis der Pioniertat, in: Datenschutz und Datensicherheit, 2/2001, S. 62.

Fox, D. (Zurück auf dem Boden, 2001):

Zurück auf dem Boden, in: Datenschutz und Datensicherheit, 8/2001, S. 442.

Freed, N. / Borenstein, N. (MIME (1) - RFC 2045, 1996):

Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies - RFC 2045, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2045.txt?number=2045 (27.12.2001).

Freed, N. / Borenstein, N. (MIME (2) - RFC 2046, 1996):

Multipurpose Internet Mail Extensions (MIME) Part Five: Media Types - RFC 2046, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2046.txt?number=2046 (27.12.2001).

Freed, N. / Borenstein, N. (MIME (5) - RFC 2049, 1996):

Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples - RFC 2049, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2049.txt?number=2049 (27.12.2001).

Freed, N. / Klensin, J. / Postel, J. (MIME (4) - RFC 2048, 1996):

Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures - RFC 2048, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2048.txt?number=2048 (27.12.2001).

Friedl, W. J. (Rechenzentrumssicherheit, 1998):
Rechenzentrumssicherheit, Berlin 1998.

Fritsch, L. (Infrastrukture for electronisc signature applications, 2001):
A secure, affordable Infrastrukture for electronisc signature applications, in: Datenschutz und Datensicherheit, 9/2001, S. 532-535.

Fuchß, T. / Fritsch, L. (Erfahrungen mit der ITSEC E4/hoch-Zertifizierung, 2000):
Erfahrungen mit der ITSEC E4/hoch-Zertifizierung, in: Datenschutz und Datensicherheit, 10/2000, S. 583-587.

Fuhrberg, K. (Internet-Sicherheit, 1998):
Internet-Sicherheit - Browser, Firewalls und Verschlüsselung, München 1998.

Garfinkel, S. / Spafford, G. (Practical Unix and Internet Security, 1996):
Practical Unix and Internet Security, 2. Aufl., Cambridge 1996.

Geiger, G. ("Information Welfare", 2000):
"Information Welfare" - Bedrohung und Schutz IT-abhängiger gesellschaftlicher Infrastrukturen, in: Datenschutz und Datensicherheit, 3/2000, S. 129-136.

Gerber, M. / Solms, R. v. (From Risk Analysis to Security Requirements, 2001):
From Risk Analysis to Security Requirements, in: Computer & Security, No. 7, S. 577-584.

Gerbich, S. (Nicht signiert, sondern resigniert, 2002):

Nicht signiert, sondern resigniert, Online im Internet unter URL: http://www.informationweek.de/index.php3?/channels/channel36/020722.htm (30.10.2002).

Gerbich, S. (Signtrust wird aufgelöst, 2002):

Signtrust wird aufgelöst, Online im Internet unter URL: http://www.informationweek.de/index.php3?/channels/channel40/021212a.htm (30.10.2002).

Geuer-Pollmann, C. / Schweitzer, N. (Vergleichbarkeit von Policies, 2000):

Vergleichbarkeit von Policies mittels XML, in: Datenschutz und Datensicherheit, 10/2000, S. 578-582.

Giessmann, E.-G. / Schmitz, R. (Zum Gültigkeitsmodell für elektronische Signaturen, 2000):

Zum Gültigkeitsmodell für elektronische Signaturen nach SigG und X.509, in: Datenschutz und Datensicherheit, 7/2000, S. 401-404.

Gollan, L. / Meinel, C. (Electronic Signatures, 2000):

Electronic Signatures - An American and European Perspective, Online im Internet unter URL: http://www.ti.fhg.de/ti-trust_center/publikationen_trustcenter/ElecSigUSEU.ps (27.12.2001).

Görg, H.-J. / Meinel, C. / Engel, T. (Konzeption einer Zertifizierungsstelle, 1997):

Trust Center - Konzeption einer Zertifizierungsstelle nach Signaturgesetz u. Signaturverordnung, Online im Internet unter URL: http://www.ti.fhg.de/ti-trust_center/publikationen_trustcenter/prep_trust.ps (27.12.2001).

Gritzalis, S. / Katsikas, S. K. / Lekkas, D. / Moulinos, K. / Polydorou, E. (The KEYSTROKE PKI Architecture, 2001):

Securing The Electronic Market: The KEYSTROKE Public Key Infrastructure Architecture, in: Computer & Security, 19, S. 731-746.

Groth, S. (Stärke multimodaler biometrischer Authentisierung, 2001):

BioID AG zeigt die Stärke multimodaler biometrischer Authentisierung auf der Systems 2001, Online im Internet unter URL: http://www.bioid.com/company/press/010813_systems_de.html (27.12.2001).

Häckelmann, H. / Petzold, H. J. / Strahringer, S. (Kommunikationssysteme, 2000):

Kommunikationssysteme, Berlin 2000.

Hammer, V. (Die 2. Dimension der IT-Sicherheit, 1999):

Die 2. Dimension der IT-Sicherheit, Braunschweig 1999.

Hammer, V. (Signaturprüfungen nach SigI, 2000):

Signaturprüfungen nach SigI, in: Datenschutz und Datensicherheit, 2/2000, S. 96-103.

Hammer, V. (Verletzlichkeitsreduzierende Technikgestaltung, 2000):
Verletzlichkeitsreduzierende Technikgestaltung, in: Datenschutz und Datensicherheit, 3/2000, S. 137-143.

Hammer, V. (Cross-Zertifikate verbinden, 2001):
Cross-Zertifikate verbinden, in: Datenschutz und Datensicherheit, 2/2001, S. 65-70.

Harnier, A. v. (Organisationsmöglichkeiten für Zertifizierungsstellen, 2000):
Organisationsmöglichkeiten für Zertifizierungsstellen nach dem Signaturgesetz, Kassel 2000.

Hartmann, M. / Maseberg, S. (Fail-Safe-Konzepte für FlexiPKI, 2002):
Fail-Safe-Konzepte für FlexiPKI, Online im Internet unter URL: http://www.informatik.tu-darmstadt.de/ftp/pub/TI/TR/TI-00-11.KSI2001_Fail_Safe_PKI_Final_Version.pdf (20.02.2002).

Hasselmann, W. (Angewandte baubetriebliche Datenverarbeitung, 2002):
Angewandte baubetriebliche Datenverarbeitung, Online im Internet unter URL: http://www.tfh-berlin.de/FB_IV/Architektur/CAD_Labor/uebung.pdf (14.03.2002).

Hastenteufel, M. / Meinel, C. (Digitale Zertifikate - Standards und Anwendungen, 1999):
Digitale Zertifikate - Standards und Anwendungen, Online im Internet unter URL: http://www.ti.fhg.de/publikationen/technische_berichte/1999/prep9901.pdf (27.12.2001).

Hattenberger, D. (Der virtuelle Behördenweg, 2001):
Der virtuelle Behördenweg, in: Datenschutz und Datensicherheit, 9/2001, S. 539-545.

Hesse, K. / Fragling, R. / Fragling, W. (Wie beurteilt man eine Bilanz?, 2000):
Wie beurteilt man eine Bilanz?, 20. Aufl., Wiesbaden 2000.

Hetschold, T. (PKI-Interoperabilität, 1999):
PKI-Interoperabilität: PKIX und SigI im Vergleich, in: Datenschutz und Datensicherheit, 4/1999, S. 213-217.

Hillebrand, A. / Bülligen, F. (Erfolgsfaktoren digitaler Signaturen, 2000):
Erfolgsfaktoren digitaler Signaturen - Eine Analyse aus sozio-ökonomischer Sicht, in: Datenschutz und Datensicherheit, 2/2000, S. 80-84.

Hoeren, T. / Schlüngel, M. (Hrsg.) (Rechtsfragen der digitalen Signatur, 1999):
Rechtsfragen der digitalen Signatur, Berlin 1999.

Höge, T. (Im Datenknast, 2001):
Im Datenknast, in: Net manager, 4/2001, S. 66-77.

Horster, P. / Kraaibeek, P. / Wohlmacher, P. (Sicherheitsinfrastrukturen - Basiskonzepte, 1999):
Sicherheitsinfrastrukturen - Basiskonzepte, Braunschweig 1999.

Hunt, R. (Technological infrastructure for PKI, 2001):
Technological infrastructure for PKI and digital certification, in: Computer Communications, 24, S. 1460-1471.

IETF Secretariat (Request for Comments, 2001):

Request for Comments, Online im Internet unter URL: http://www.ietf.org/rfc.html (27.12.2001).

Jahnke, H. (Erfahrungskurve, 2002):

Erfahrungskurve, in: Küpper, H.-U. / Wagenhofer, A. (Hrsg.), Handwörterbuch der Unternehmensrechnung und Controlling, 4. Aufl., Stuttgart, 2000, Sp. 384-392.

Kelly, K. (New Rules for the New Economy, 1998):

New Rules for the New Economy - 10 Radical Strategies for a connected World, New York 1998.

Kelm, S. (Signed in Germany, 1999):

Signed in Germany, in: Datenschutz und Datensicherheit, 9/1999, S. 526-528.

Key Recovery Alliance (Technology Papers, Special Issue - Introduction, 2000):

Technology Papers, Special Issue - Introduction, in: Computer & Security, No. 1, S. 18-19.

Kienbaum Management Consultants GmbH (IT-Gehälter in Europa, 2002):

Neue Kienbaum-Studie vergleicht die IT-Gehälter in Europa, Online im Internet unter URL: http://www.kienbaum.de/ (25.07.2002).

Kienbaum Management Consultants GmbH (IT-Gehälter stagnieren, 2002):

IT-Gehälter stagnieren Fachkräfte weiter gefragt, Online im Internet unter URL: http://www.kienbaum.de/ (25.07.2002).

Kilger, W. (Einführung in die Kostenrechnung, 1987):

Einführung in die Kostenrechnung, 3. Aufl., Wiesbaden 1987.

Kilger, W. (Flexible Plankostenrechnung, 1993):

Flexible Plankostenrechnung und Deckungsbeitragsrechnung, 10. Aufl., Wiesbaden 1993.

Klau, A. (Globalisierung, 1999):

Globalisierung - Definition, Bestimmungsgründe, Auswirkungen, Online im Internet unter URL: www.vwl.uni-freiburg.de/fakultaet/moe/forschung/globalisierung.pdf (23.02.2002).

Kobil Systems GmbH (Chipkartenterminals, 2002):

Chipkartenterminals, Online im Internet unter URL: http://www.kobil.de/seiten/d/ct.htm (29.07.2002).

Kowol, G. (Primzahlen, 1995):

Primzahlen - Ein mathematischer Zugang zu ihren Qualitäten, Dornach 1995.

Krempl, S. (Signatur Schlamassel, 2002):

Signatur Schlamassel - Wer hilft der digitalen Signatur aus der Krise: Industrie oder Politik?, in: c't, Heft 13/2002, S. 47.

Kühn, U. (Technische Grundlagen, 1999):

Technische Grundlagen digitaler Signaturverfahren, in: Hoeren, T. / Schlüngel, M. (Hrsg.), Rechtsfragen der digitalen Signatur, S. 65-92.

Kuhner, C. (Rentabilität, 2002):

Rentabilität, in: Küpper, H.-U. / Wagenhofer, A. (Hrsg.), Handwörterbuch der Unternehmensrechnung und Controlling, 4. Auflage, Stuttgart, 2002, Sp. 1695-1702.

Kuner, C. (Signaturgesetz und "Political Correctness", 1999):

Signaturgesetz und "Political Correctness", in: Datenschutz und Datensicherheit, 4/1999, S. 227-228.

Kyas, O. (Sicherheit im Internet, 1998):

Sicherheit im Internet, Bonn 1998.

Langenbach, C. J. / Ulrich, O. (Hrsg.) (Elektronische Signaturen, 2002):

Elektronische Signaturen, Berlin 2002.

Lehrstuhl Theoretische Informatik, TU Darmstadt (FlexiPKI, 2001):

FlexiPKI - Flexible Public-Key-Infrastrukturen, Online im Internet unter URL: http://www.informatik.tu-darmstadt.de/TI/Forschung/FlexiPKI/Welcome.html (27.12.2001).

Leistenschneider, M. (Aufbau einer SigG-konformen Zertifizierungsstelle, 2001):

Aufbau einer SigG-konformen Zertifizierungsstelle, Online im Internet unter URL: http://www.secorvo.de/pki-symposium/symposium-2001/leistenschneider011010.pdf (27.12.2001).

Lenstra, A. K. / Verheul, E. R. (Selecting Cryptographic Key Sizes, 2000):

Selecting Cryptographic Key Sizes, in: Datenschutz und Datensicherheit, 3/2000, S. 166.

Mack, H. (Sperren von Zertifikaten, 2001):

Sperren von Zertifikaten in der Praxis - eine Fallanalyse, in: Datenschutz und Datensicherheit, 8/2001, S. 464-466.

Meeker, M. / Pearson, S. (The Internet Retailing Report, 1997):

The Internet Retailing Report, Online im Internet unter URL: www.ms.com (11.12.2001).

Mellerowicz, K. (Kosten und Kostenrechnung, 1973):

Kosten und Kostenrechnung, 5. Aufl., Berlin 1973.

Merz, M. (Electronic Commerce, 1999):

Electronic Commerce - Marktmodell, Anwendungen und Technologien, Heidelberg 1999.

Miedbrodt, A. (US-amerikanische Signaturgesetze, 1998):

Anwendungserfahrungen ausgewählter US-amerikanischer Signaturgesetze, in: Datenschutz und Datensicherheit, 4/1998, S. 194-198.

Ministerium für Arbeit und Bau (Preisindexzahl für Rohbauwerte, 2002):

Baugebührenordnung; Preisindexzahl für Rohbauwerte, Online im Internet unter URL: http://www.am.mv-regierung.de/arbm/pages/BO_BauGO_preisindex.htm (14.03.2002).

Moore, G. E. (Components onto integrated circuits, 1965):

Cramming more components onto integrated circuits, in: Electronics, 8/1965, S. 114-117.

Moore, K. (MIME (3) - RFC 2047, 1996):

MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text - RFC 2047, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2047.txt?number=2047 (27.12.2001).

Müller, H. B. / Roessler, T. (Rechtlichen Anerkennung elektronischer Signaturen, 1999):

Zur rechtlichen Anerkennung elektronischer Signaturen in Europa, in: Datenschutz und Datensicherheit, 9/1999, S. 497-502.

Nechvatal, J. / Barker, E. / Bassham, L. / Burr, W. / Dworkin, M. / Foti, J. / Roback, E. (Advanced Encryption Standard (AES), 2000):

Report on the Development of the Advanced Encryption Standard (AES), Online im Internet unter URL: http://csrc.nist.gov/encryption/aes/round2/r2report.pdf (27.12.2001).

n-tv (KPNQwest: Konkurs angemeldet, 2002):

KPNQwest: Konkurs angemeldet, Online im Internet unter URL: http://www.n-tv.de/3016791.html (29.07.2002).

n-tv (WorldCom beantragt Insolvenz, 2002):

WorldCom beantragt Insolvenz, Online im Internet unter URL: http://www.n-tv.de/3052009.html (29.07.2002).

o.V. (Digitale Signatur dank Isis-MTT auf dem Sprung, 2001):

Digitale Signatur dank Isis-MTT auf dem Sprung, in: Computerwoche, 49/2001, S. 37.

o.V. (How PGP works, 2001):

How PGP works, Online im Internet unter URL: http://www.pgpi.org/doc/pgpintro/ (27.12.2001).

o.V. (Investitionskosten beim Aufbau eines Call Centers, 2001):

Investitionskosten beim Aufbau eines Call Centers, Online im Internet unter URL: http://www.call-center-24.de/calldeutsch/CCNeugrunder/Checkliste/controlling.html (27.12.2001).

o.V. (PGP, 2001):

PGP, Online im Internet unter URL: http://www.pgp.com/ (27.12.2001).

o.V. (Webopedia, 2001):

Webopedia, Online im Internet unter URL: http://www.webopedia.com/ (27.12.2001).

o.V. ("Aus" des TrustCenter-Geschäftes bei der POST AG, 2002):

Erste Reaktionen zum "Aus" des TrustCenter-Geschäftes bei der POST AG, Online im Internet unter URL: http://www.content-corner.de/show/705547511/show.asp?p=3986&c=site.css (30.10.2002).

o.V. (Markt noch nicht reif, 2002):

Für die qualifizierte Signatur ist der Markt noch nicht reif, in: Computer Zeitung, 33. Jahrgang, Nr. 23, S. 1.

o.V. (T-Online secureMail, 2002):

T-Online secureMail, Online im Internet unter URL: http://dienste.t-online-business.de/busi/dien/sich/mail/ar/ar-preise,iID=494582,frame=cont.html (30.12.2002).

Oertel, K. (Elektronische Form und notarielle Aufgaben, 2001):

Elektronische Form und notarielle Aufgaben im elektronischen Rechtsverkehr, in: Multimedia und Recht, 7/2001, S. 419-423.

Paar, C. (Algorithmenunabhängige Krypto-Hardware, 1999):

Algorithmenunabhängige Krypto-Hardware, in: Datenschutz und Datensicherheit, 10/1999, S. 562-564.

Paulus, S. (Rundum-sorglos Paket mit Hindernissen, 2001):

Rundum-sorglos Paket mit Hindernissen, in: Datenschutz und Datensicherheit, 9/2001, S. 529-531.

Perlman, R. (An Overview of PKI Trust Models, 1999):

An Overview of PKI Trust Models, in: IEEE Network, November/Dezember 1999, S. 38-43.

Picot, A. (Zehn Eigenschaften der Internet-Ökonomie, 2001):

Zehn Eigenschaften der Internet-Ökonomie, Online im Internet unter URL: www.competence-site.de/ebusiness.nsf/9A49EFF5CEE4D033C125697A005B4FFD/$File/eigenschaften_der_internet_ökonomie.pdf (20.02.2002).

Picot, A. / Reichwald, R. / Wigand, R. T. (Die grenzlose Unternehmung, 2001):

Die grenzlose Unternehmung - Information, Organisation und Management, 4. Aufl., Wiesbaden 2001.

PKIX Working Group (Webseite der PKIX Working Group, 2001):

Webseite der PKIX Working Group, Online im Internet unter URL: http://www.imc.org/ietf-pkix/index.html (27.12.2001).

Pordesch, U. (Der fehlende Nachweis, 2000):

Der fehlende Nachweis der Präsentation signierter Daten, in: Datenschutz und Datensicherheit, 2/2000, S. 89-95.

Postel, J. (IP - RFC 791, 1981):

Internet Protokoll (IP) - RFC 791, Online im Internet unter URL: http://www.ietf.org/rfc/rfc0791.txt?number=791 (27.12.2001).

Postel, J. (TCP - RFC 793, 1981):

Transmission Control Protokoll (TCP) - RFC 793, Online im Internet unter URL: http://www.ietf.org/rfc/rfc0793.txt?number=793 (27.12.2001).

Postel, J. (SMTP - RFC 821, 1982):

Simple Mail Transfer Protokoll (SMTP) - RFC 821, Online im Internet unter URL: http://www.ietf.org/rfc/rfc0821.txt?number=821 (14.07.2002).

Purser, S. (A Simple Graphical Tool For Modelling Trust, 2001):

A Simple Graphical Tool For Modelling Trust, in: Computer & Security, No. 6, S. 479-484.

Raepple, M. (Sicherheitskonzepte für das Internet, 2001):

Sicherheitskonzepte für das Internet, 2. Aufl., Heidelberg 2001.

Raepple, M. (Sicherheit in elektronischen Märkten, 2002):

Sicherheit in elektronischen Märkten, in: Handbuch der maschinellen Datenverarbeitung, HMD 223, Februar 2002, S. 63-75.

Rainbow Technologies (iKey 2000, 2001):

eSecurity für eBusiness - iKey 2000, Online im Internet unter URL: http://www.rainbow.de/ikey/ikey2000.html (27.12.2001).

Ramsdell, B. (S/MIME - RFC 2633, 1999):

S/MIME Version 3 Message Specification (S/MIME) - RFC 2633, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2633.txt?number=2633 (27.12.2001).

Ranneberg, K. (Zertifizierung mehrseitiger IT-Sicherheit, 1998):

Zertifizierung mehrseitiger IT-Sicherheit - Kriterien und organisatorische Rahmenbedingungen, Braunschweig 1998.

Ring Deutscher Makler - Bundesverbandes (RDM-Immobilien-Preisspiegel 2001, 2001):

RDM-Immobilien-Preisspiegel 2001, Online im Internet unter URL: http://www.rdm.de - Informationsforum - Presispiegel (14.03.2002).

Regulierungsbehörde für Telekommunikation und Post (Elektronische Signaturen - FAQ, 2002):

Elektronische Signaturen - FAQ, Online im Internet unter URL: http://www.regtp.de/tech_reg_tele/start/in_06-02-03-00-00_m/index.html (31.01.2002).

Regulierungsbehörde für Telekommunikation und Post (BSI-Handbuch für digitale Signaturen, 1997):
BSI-Handbuch für digitale Signaturen, Online im Internet unter URL:
http://www.bsi.bund.de/esig/basics/techbas/masskat/bsikat.pdf (25.07.2002).

Regulierungsbehörde für Telekommunikation und Post (Zertifizierungsdiensteanbieter, 2002):
Zertifizierungsdiensteanbieter, Online im Internet unter URL: http://www.regtp.de/tech_reg_tele/start/in_06-02-04-00-00_m/index.html (20.08.2002).

Reif, H. (Bridge-CA, 2001):
Bridge-CA, in: Datenschutz und Datensicherheit, 9/2001, S. 553.

Rescorla, E. / Schiffman, A (S-HTTP - RFC 2660, 1999):
The Secure HyperText Transfer Protocol (S-HTTP) - RFC 2660, Online im Internet unter URL: http://www.ietf.org/rfc/rfc2660.txt?number=2660 (27.12.2001).

Rieß, J. (Signaturgesetz - Der Markt ist unsicher, 2000):
Signaturgesetz - Der Markt ist unsicher, in: Datenschutz und Datensicherheit, 9/2000, S. 530-534.

Rivest, R. L. (MD4 - RFC 1320, 1992):
The MD4 Message-Digest Algorithm (MD4) - RFC 1320, Online im Internet unter URL: http://www.ietf.org/rfc/rfc1320.txt?number=1320 (27.12.2001).

Rivest, R. L. (MD5 - RFC 1321, 1992):

The MD5 Message-Digest Algorithm (MD5) - RFC 1321, Online im Internet unter URL: http://www.ietf.org/rfc/rfc1321.txt?number=1321 (27.12.2001).

Rivest, R. L. / Shamir, A. / Adleman, L. (A Method for Obtaining Public-Key Cryptosystems, 1978):

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Online im Internet unter URL: http://theory.lcs.mit.edu/~rivest/rsapaper.pdf (27.12.2001).

Robben, M. (Digitale Signatur, 2000):

Digitale Signatur - Auftrieb für den E-Commerce?, Online im Internet unter URL: http://www.ecin.de/sicherheit/signatur/ (27.12.2001).

Röhm, A. W. (Sicherheit offener Elektronischer Märkte, 2000):

Sicherheit offener Elektronischer Märkte - Modellbildung und Realisierungskonzept, Lohmar 2000.

Rose, M. (POP3 - RFC 1081, 1988):

Post Office Protocol - Version 3 (POP3) - RFC 1081, Online im Internet unter URL: http://www.ietf.org/rfc/rfc1081.txt?number=1081 (14.07.2002).

Ross, D. E. (PGP: Backdoors and Key Escrow, 2001):

PGP: Backdoors and Key Escrow, Online im Internet unter URL: http://www.vcnet.com/~rossde/pgp_backdoor.html (27.12.2001).

Roßnagel, A. (Elektronsiche Signaturen in Europa, 1998):

Elektronsiche Signaturen in Europa, in: Multimedia und Recht, 7/1998, S. 331-337.

Roßnagel, A. (Europäische Signatur-Richtlinie, 1999):

Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung, in: Multimedia und Recht, 5/1999, S. 261-266.

Roßnagel, A. (Das neue Signaturgesetz, 2001):

Das neue Signaturgesetz - Grundlage des elektronischen Rechtsverkehrs, in: Multimedia und Recht, 4/2001, S. 201-202.

Rötzer, F. (ECommerce-Websites lahmgelegt, 2000):

ECommerce-Websites lahmgelegt, Online im Internet unter URL: http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=5766&rub_ordner=inhalt (09.02.2000).

RSA Security Inc (What are SHA and SHA-1?, 2002):

What are SHA and SHA-1?, Online im Internet unter URL: http://www.rsasecurity.com/rsalabs/faq/3-6-5.html (25.07.2002).

Rupp, S. (Call Center Praxis, 2000):

Call Center Praxis: so bringen Sie Ihren Vertrieb voran, 2. Aufl., Neuwied 2000.

Russell, R. / Cunningham, S. (Maximum Protection, 2001):

Maximum Protection, Bonn 2001.

Schmeh, K. (Kryptographie, 2001):

Kryptographie und Public-Key-Infrastrukturen im Internet, 2. Aufl., Heidelberg 2001.

Schmid, G. (ECHOLON, 2001):

Entwurf eines Berichts über die Existenz eines globalen Abhörsystemns (ECHOLON), Online im Internet unter URL: http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_de.pdf (12.12.2001).

Schmidt, J. (Virenbasteln für Dummies, 2001):

Virenbasteln für Dummies, in: c't, Heft 13/2001, S. S. 99-101.

Schneider, D. (E-Shopping, 1999):

E-Shopping - Erfolgsstrategien im electronic commerce, Wiesbaden 1999.

Schneier, B. (Applied Cryptography, 1996):

Applied Cryptography, 2. Aufl., New York 1996.

Schneier, F. B. (trust in cyberspace, 1999):

trust in cyberspace, Washington 1999.

Schneier, B. (Secret & Lies, 2001):

Secret & Lies - IT-Sicherheit in einer vernetzten Welt, Heidelberg 2001.

Schuhmacher, J. (Wirtschafts- und Wettbewerbsspionage, 2001):

Wirtschafts- und Wettbewerbsspionage, Online im Internet unter URL: http://www.internet21.de/artikel/spionage.htm (27.12.2001).

Schultz, E. E. / Proctor, R. W. / Lien, M.-C. / Salvendy, G. (Usability and Security, 2001):
Usability and Security - An Appraisal of Usability Issus in Information Security Methods, in: Computer & Security, No. 7, S. 620-634.

Schürer, T. (Zentrale PKI-Lösungen, 2000):
Zentrale PKI-Lösungen und deren Anwendung in TrustServices, in: Datenschutz und Datensicherheit, 10/2000, S. 573-577.

Schweitzer, M. / Küpper, H.-U. (Systeme der Kosten- und Erlösrechnung, 1998):
Systeme der Kosten- und Erlösrechnung, 7. Aufl., München 1998.

Schwemmer, J. (Frontbericht 1.0, 2000):
Frontbericht 1.0 - Der steinige Weg zur digitalen Unterschrift, in: Datenschutz und Datensicherheit, 2/2000, S. 70-73.

Schwemmer, J. ((Why) It's a long Way to Interoperability, 2001):
Solutions and Problems - (Why) It's a long Way to Interoperability, in: Datenschutz und Datensicherheit, 9/2001, S. 526-528.

SecCommerce Informationssysteme GmbH (Smartcards: Physikalische Sicherheit, 2001):
Smartcards: Physikalische Sicherheit, Online im Internet unter URL:
http://www.seccommerce.de/de/fachwissen/technologie/smartcards/smartcards_physikalische_sicherheit.html (27.12.2001).

Selke, G. (Kryptographie, 2000):

Kryptographie - Verfahren, Ziele, Einsatzmöglichkeiten, Köln 2000.

Senderek, R. (How PGP deals With Manipulated Keys, 2000):

How PGP deals With Manipulated Keys, in: Datenschutz und Datensicherheit, 10/2000, S. 603-608.

Singh, S. (Geheime Botschaften, 2000):

Geheime Botschaften, München 2000.

Singh, S. (Fermats letzter Satz, 2001):

Fermats letzter Satz, 6. Aufl., München 2001.

Smith, R. E. (Internet Kryptographie, 1998):

Internet Kryptographie, Bonn 1998.

SOMMER Systemtechnik (Webseiten von SOMMER Systemtechnik, 2002):

Webseiten von SOMMER Systemtechnik, Online im Internet unter URL: http://www.sommer-hof.de/ (29.07.2002).

Stark, C. / Biester, J. / Fell, H.-W. / Volk, D. u.a. (PKI Organisationshandbuch, 2001):

PKI Organisationshandbuch (Version 4.1 vom 25.01.2001), Online im Internet unter URL: http://www.secorvo.de/publikat/sphinx-orghbv4.1.zip (27.12.2001).

Stumm, F.-S. / Weber, F. (Infrastruktur für Zertifizierungsstellen, 2000):
Maßnahmeempfehlungen: Infrstruktur für Zertifizierungsstellen (SigG/SigV), Online im Internet unter URL: http://www.bsi.de/esig/lit/tcinfra.pdf (27.12.2001).

T7 Organisation (Webseite der T7 Organisation, 2001):
Webseite der T7 Organisation, Online im Internet unter URL: http://www.t7-isis.de/ (27.12.2001).

T7-ISIS Organisation (ISIS-MTT 1.01 Release, 2001):
ISIS-MTT 1.01 Release, Online im Internet unter URL: http://www.t7-isis.de/ISIS-MTT/isis-mtt.html (27.12.2001).

Taeger, J. (Rechtssichere Gestaltung, 2002):
Rechtssichere Gestaltung des elektronischen Geschäftsverkehrs, in: Tagungsband: Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung, xxx, S. 129-143.

Tanenbaum, A. S. (Moderne Betriebssysteme, 1995):
Moderne Betriebssysteme, 2. Aufl., München 1995.

Tanenbaum, A. S. (Computernetzwerke, 2000):
Computernetzwerke, 3. Aufl., München 2000.

Teufel, S. / Schlienger, T. (Informationssicherheit, 2000):
Informationssicherheit - Wege zur kontrollierten Unsicherheit, in: Praxis der Wirtschaftsinformatik, 216, S. 18-31.

Thiel, C. (Internationale Public-Key-Infrastrukturen, 2000):
Internationale Public-Key-Infrastrukturen aus Nutzersicht, in: Datenschutz und Datensicherheit, 9/2000, S. 523-526.

Thiel, C. (Marktentwicklung im Umfeld digitaler Signaturen, 2000):

Marktentwicklung im Umfeld digitaler Signaturen, in: Datenschutz und Datensicherheit, 2/2000, S. 77-79.

Tiscali Business GmbH (Tiscali.host, 2001):

Tiscali.host, Online im Internet unter URL: http://62.27.91.84/download/get_file.phix/host.pdf?session=6cadce9e5566e4af2d0bad24efeb21b1&id=c46f96c66dee62a55f2137ff7f9fabeb (27.12.2001).

Verband Deutscher Makler (Gewerbepreisspiegel 2001, 2001):

Gewerbepreisspiegel 2001, Online im Internet unter URL: http://www.vdm.de/bundespreisspiegel/ (01.08.2002).

Welsch, G. (Stufenweise skalierbare Sicherheit, 1999):

Stufenweise skalierbare Sicherheit für digitale Signaturen, in: Datenschutz und Datensicherheit, 9/1999, S. 520-525.

Welsch, G. (Das Signaturänderungsgesetz, 2000):

Das Signaturänderungsgesetz, in: Datenschutz und Datensicherheit, 7/2000, S. 408-414.

Welsch, G. / Bremer, K. (Die europäische Signaturrichtlinie in der Praxis, 2000):

Die europäische Signaturrichtlinie in der Praxis, in: Datenschutz und Datensicherheit, 2/2000, S. 85-88.

Welschenbach, M. (Rijndael - Nachfolger des DES, 2001):

Rijndael - Nachfolger des DES, in: Datenschutz und Datensicherheit, 6/2001, S. 317-322.

Westermann, D. (Neuer eBusiness-Service, 2000):

Neuer eBusiness-Service der Deutschen Post Com - Die elektronische Rechnung im Web, Online im Internet unter URL: http://www.dpcom.de/WebStar5/DPCOM/WS50_DPCOM.nsf/WebReferView/-WebPages-_Pressemitteilungen_Daten_04.10.2000 (12.12.2001).

Wiesner, B. (Key Recovery, 2000):

Key Recovery, in: Datenschutz und Datensicherheit, 12/2000, S. 698-703.

Wilkens, A. (Deutsche Post ohne Online-Geschäft, 2002):

Deutsche Post ohne Online-Geschäft, in: c't, 12/2002, S. 43.

Wirtz, B. W. (Medien- und Internetmanagement, 2000):

Medien- und Internetmanagement, Wiesbaden 2000.

Wobst, R. (Abenteuer Kryptologie, 1998):

Abenteuer Kryptologie - Methoden, Risiken und Nutzen der Datenverschlüsselung, 2. Aufl., München 1998.

Wohlmacher, P. (Digitale Signaturen und Sicherheitsinfrastrukturen, 2001):

Digitale Signaturen und Sicherheitsinfrastrukturen, Höhenkirchen 2001.

Zerdick et al. (Die Internet-Ökonomie, 2001):

Die Internet-Ökonomie - Strategien für die digitale Wirtschaft, 3. Aufl., Berlin 2001.

Zimmermann, G. (Grundzüge der Kostenrechnung, 1985):

Grundzüge der Kostenrechnung, 3. Aufl., Stuttgart 1985.

Zimmermann, P. (Message from Phil Zimmermann, Creator of PGP, 2000): Message from Phil Zimmermann, Creator of PGP, Online im Internet unter URL: http://www.pgp.com/support/product-advisories/phil-message.asp (27.12.2001).

Anhang

Europäische Signaturrichtlinie

Im folgenden die RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13.Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 13. Dezember 1999
über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 47 Absatz 2, Artikel 55 und 95,

auf Vorschlag der Kommission [1],

nach Stellungnahme des Wirtschafts- und Sozialausschusses [2],

nach Stellungnahme des Ausschusses der Regionen [3],

gemäß dem Verfahren des Artikels 251 des Vertrags [4],

in Erwägung nachstehender Gründe:

(1) Am 16. April 1997 hat die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen eine Mitteilung mit dem Titel „Europäische Initiative für den elektronischen Geschäftsverkehr" vorgelegt.

(2) Am 8. Oktober 1997 hat die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen eine Mitteilung über „Sicherheit und Vertrauen in elektronische Kommunikation — Ein europäischer Rahmen für digitale Signaturen und Verschlüsselung" unterbreitet.

(3) Am 1. Dezember 1997 hat der Rat die Kommission aufgefordert, so bald wie möglich einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über digitale Signaturen vorzulegen.

(4) Elektronische Kommunikation und elektronischer Geschäftsverkehr erfordern „elektronische Signaturen" und entsprechende Authentifizierungsdienste für Daten. Divergierende Regeln über die rechtliche Anerkennung elektronischer Signaturen und die Akkreditierung von Zertifizierungsdiensteanbietern in den Mitgliedstaaten können ein ernsthaftes Hindernis für die elektronische Kommunikation und den elektronischen Geschäftsverkehr darstellen. Klare gemeinschaftliche Rahmenbedingungen für elektronische Signaturen stärken demgegenüber das Vertrauen und die allgemeine Akzeptanz hinsichtlich der neuen Technologien. Die Rechtsvorschriften der Mitgliedstaaten sollten den freien Waren- und Dienstleistungsverkehr im Binnenmarkt nicht behindern.

(5) Die Interoperabilität von Produkten für elektronische Signaturen sollte gefördert werden. Gemäß Artikel 14 des Vertrags umfaßt der Binnenmarkt einen Raum ohne Binnengrenzen, in dem der freie Warenverkehr gewährleistet ist. Es sind grundlegende Anforderungen zu erfüllen, die speziell für Produkte für elektronische Signaturen gelten, um so den freien Verkehr im Binnenmarkt zu gewährleisten und das Vertrauen in digitale Signaturen zu fördern, wobei die Verordnung (EG) Nr. 3381/94 des Rates vom 19. Dezember 1994 über eine Gemeinschaftsregelung der Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck [5] und der Beschluß 94/942/GASP des Rates vom 19. Dezember 1994 über die vom Rat angenommene gemeinsame Aktion zur Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck [6] unberührt bleiben.

(6) Mit der vorliegenden Richtlinie wird die Erbringung von Dienstleistungen im Bereich der Vertraulichkeit von Informationen nicht harmonisiert, wenn für derartige Dienstleistungen einzelstaatliche Vorschriften hinsichtlich der öffentlichen Ordnung oder Sicherheit gelten.

(7) Der Binnenmarkt gewährleistet die Freizügigkeit von Personen, wodurch Bürger und Gebietsansässige der Europäischen Union zunehmend mit Stellen in anderen Mitgliedstaaten als demjenigen ihres Wohnsitzes in Verbindung treten müssen. Die Möglichkeit der elektronischen Kommunikation könnte in dieser Hinsicht von großem Nutzen sein.

(8) Die rasche technologische Entwicklung und der globale Charakter des Internet erfordern ein Konzept, das verschiedenen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offensteht.

(9) Elektronische Signaturen werden bei einer Vielzahl von Gegebenheiten und Anwendungen genutzt, die zu einem großen Spektrum neuer Dienste und Produkte im Zusammenhang mit oder unter Verwendung von elektronischen Signaturen führen. Die Definition solcher Produkte und Dienste sollte sich nicht auf die Ausstellung und Verwaltung von Zertifikaten beschränken, sondern sollte auch alle sonstigen Dienste und Produkte einschließen, die elektronische Signaturen verwenden oder mit ihnen zusammenhängen, wie Registrierungsdienste, Zeitstempel, Verzeichnisdienste, Rechnerdienste oder Beratungsdienste in Verbindung mit elektronischen Signaturen.

(10) Der Binnenmarkt ermöglicht es Zertifizierungsdiensteanbietern, grenzüberschreitend tätig zu werden, um ihre Wettbewerbsfähigkeit zu steigern und damit Verbrauchern und Unternehmen ohne Rücksicht auf Grenzen neue Möglichkeiten des sicheren Informationsaustausches und elektronischen Geschäftsverkehrs zu eröffnen. Um das gemeinschaftsweite Anbieten von Zertifizierungsdiensten über offene Netze zu fördern, sollten Anbieter von Zertifizierungsdiensten diese ungehindert ohne vorherige Genehmigung bereitstellen können.

[1] ABl. C 325 vom 23.10.1998, S. 5.
[2] ABl. C 40 vom 15.2.1999, S. 29.
[3] ABl. C 93 vom 6.4.1999, S. 33.
[4] Stellungnahme des Europäischen Parlaments vom 13. Januar 1999 (ABl. C 104 vom 14.4.1999, S. 49). Gemeinsamer Standpunkt des Rates vom 28. Juni 1999 (ABl. C 243 vom 27.8.1999, S. 33) und Beschluß des Europäischen Parlaments vom 27. Oktober 1999 (noch nicht im Amtsblatt veröffentlicht). Beschluß des Rates vom 30. November 1999.

[5] ABl. L 367 vom 31.12.1994, S. 1. Verordnung geändert durch die Verordnung (EG) Nr. 837/95 (ABl. L 90 vom 21.4.1995, S. 1).
[6] ABl. L 367 vom 31.12.1994, S. 8. Beschluß zuletzt geändert durch den Beschluß 1999/193/GASP (ABl. L 73 vom 19.3.1999, S. 1).

Vorherige Genehmigung bedeutet nicht nur eine Erlaubnis, wonach der betreffende Zertifizierungsdiensteanbieter einen Bescheid der einzelstaatlichen Stellen einholen muß, bevor er seine Zertifizierungsdienste erbringen kann, sondern auch alle sonstigen Maßnahmen mit der gleichen Wirkung.

(11) Freiwillige Akkreditierungssysteme, die auf eine Steigerung des Niveaus der erbrachten Dienste abzielen, können Zertifizierungsdiensteanbietern den geeigneten Rahmen für die Weiterentwicklung ihrer Dienste bieten, um das auf dem sich entwickelnden Markt geforderte Maß an Vertrauen, Sicherheit und Qualität zu erreichen. Diese Systeme sollten die Entwicklung bester Praktiken durch Zertifizierungsdiensteanbieter fördern. Zertifizierungsdiensteanbietern sollte es freistehen, sich akkreditieren zu lassen und Akkreditierungssysteme zu nutzen.

(12) Zertifizierungsdienste sollten entweder von einer öffentlichen Stelle oder einer juristischen oder natürlichen Person angeboten werden können, sofern diese im Einklang mit den einzelstaatlichen Rechtsvorschriften niedergelassen ist. Die Mitgliedstaaten sollten es Anbietern von Zertifizierungsdiensten nicht untersagen, auch ohne freiwillige Akkreditierung tätig zu sein. Es ist darauf zu achten, daß Akkreditierungssysteme den Wettbewerb im Bereich der Zertifizierungsdienste nicht einschränken.

(13) Die Mitgliedstaaten können entscheiden, wie sie die Überwachung der Einhaltung der Bestimmungen dieser Richtlinie gewährleisten. Diese Richtlinie schließt nicht aus, daß privatwirtschaftliche Überwachungssysteme geschaffen werden. Diese Richtlinie verpflichtet die Zertifizierungsdiensteanbieter nicht, eine Überwachung im Rahmen eines geltenden Akkreditierungssystems zu beantragen.

(14) Es ist wichtig, ein ausgewogenes Verhältnis zwischen den Bedürfnissen der Verbraucher und der Unternehmen herzustellen.

(15) Anhang III enthält die Anforderungen für sichere Signaturerstellungseinheiten zur Gewährleistung der Funktionalität fortgeschrittener elektronischer Signaturen. Er deckt nicht die gesamte Systemumgebung ab, in der die Einheit betrieben wird. Das Funktionieren des Binnenmarktes verlangt von der Kommission und den Mitgliedstaaten, rasch zu handeln, damit die Stellen benannt werden können, die für die Bewertung der Übereinstimmung von sicheren Signaturerstellungseinheiten mit den Anforderungen des Anhangs III zuständig sind. Um den Markterfordernissen zu entsprechen, muß die Bewertung der Übereinstimmung rechtzeitig und effizient erfolgen.

(16) Diese Richtlinie leistet einen Beitrag zur Verwendung und rechtlichen Anerkennung elektronischer Signaturen in der Gemeinschaft. Es bedarf keiner gesetzlichen Rahmenbedingungen für elektronische Signaturen, die ausschließlich in Systemen verwendet werden, die auf freiwilligen privatrechtlichen Vereinbarungen zwischen einer bestimmten Anzahl von Teilnehmern beruhen. Die Freiheit der Parteien, die Bedingungen zu vereinbaren, unter denen sie elektronisch signierte Daten akzeptieren, sollte respektiert werden, soweit dies im Rahmen des innerstaatlichen Rechts möglich ist. Elektronischen Signaturen, die in solchen Systemen verwendet werden, sollte die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht abgesprochen werden.

(17) Diese Richtlinie zielt nicht darauf ab, nationales Vertragsrecht, insbesondere betreffend den Abschluß und die Erfüllung von Verträgen, oder andere, außervertragliche Formvorschriften bezüglich der Unterschriften zu harmonisieren. Deshalb sollten die Regelungen über die rechtliche Wirksamkeit elektronischer Signaturen unbeschadet einzelstaatlicher Formvorschriften gelten, die den Abschluß von Verträgen oder die Festlegung des Ortes eines Vertragsabschlusses betreffen.

(18) Das Speichern und Kopieren von Signaturerstellungsdaten könnte die Rechtsgültigkeit elektronischer Signaturen gefährden.

(19) Elektronische Signaturen werden im öffentlichen Bereich innerhalb der staatlichen und gemeinschaftlichen Verwaltungen und im Kommunikationsverkehr zwischen diesen Verwaltungen sowie zwischen diesen und den Bürgern und Wirtschaftsteilnehmern eingesetzt, z. B. in den Bereichen öffentliche Auftragsvergabe, Steuern, soziale Sicherheit, Gesundheit und Justiz.

(20) Durch harmonisierte Kriterien im Zusammenhang mit der Rechtswirkung elektronischer Signaturen läßt sich gemeinschaftsweit ein kohärenter Rechtsrahmen aufrechterhalten. In den einzelstaatlichen Rechtsvorschriften sind verschiedene Anforderungen für die Rechtsgültigkeit handschriftlicher Unterschriften niedergelegt. Zertifikate können dazu dienen, die Identität einer elektronisch signierenden Person zu bestätigen. Auf qualifizierten Zertifikaten beruhende fortgeschrittene elektronische Signaturen zielen auf einen höheren Sicherheitsstandard. Fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt werden, können nur dann gegenüber handschriftlichen Unterschriften als rechtlich gleichwertig angesehen werden, wenn die Anforderungen für handschriftliche Unterschriften erfüllt sind.

(21) Um die allgemeine Akzeptanz elektronischer Authentifizierungsmethoden zu fördern, ist zu gewährleisten, daß elektronische Signaturen in allen Mitgliedstaaten in Gerichtsverfahren als Beweismittel verwendet werden können. Die rechtliche Anerkennung elektronischer Signaturen sollte auf objektiven Kriterien beruhen und nicht mit einer Genehmigung für den betreffenden Zertifizierungsdiensteanbieter verknüpft sein. Die Festlegung der Rechtsgebiete, in denen elektronische Dokumente und elektronische Signaturen verwendet werden können, unterliegt einzelstaatlichem Recht. Diese Richtlinie läßt die Befugnis der einzelstaatlichen Gerichte, über die Übereinstimmung mit den Anforderungen dieser Richtlinie zu befinden, unberührt; sie berührt auch nicht die einzelstaatlichen Vorschriften über die freie gerichtliche Würdigung von Beweismitteln.

(22) Diensteanbieter, die ihre Zertifizierungsdienste öffentlich anbieten, unterliegen den einzelstaatlichen Haftungsregelungen.

(23) Die Entwicklung des internationalen elektronischen Geschäftsverkehrs erfordert grenzüberschreitende Vereinbarungen unter Beteiligung von Drittländern. Um die weltweite Interoperabilität zu gewährleisten, könnten Vereinbarungen mit Drittländern über multilaterale Regeln betreffend die gegenseitige Anerkennung der Zertifizierungsdienste nützlich sein.

(24) Zur Stärkung des Vertrauens der Nutzer in die elektronische Kommunikation und den elektronischen Geschäftsverkehr müssen die Zertifizierungsdiensteanbieter die Vorschriften über den Datenschutz und den Schutz der Privatsphäre achten.

(25) Die Bestimmungen über die Nutzung von Pseudonymen in Zertifikaten hindern die Mitgliedstaaten nicht daran, eine Identifizierung der Personen nach Gemeinschaftsrecht oder einzelstaatlichem Recht zu verlangen.

(26) Die zur Durchführung dieser Richtlinie erforderlichen Maßnahmen sind gemäß Artikel 2 des Beschlusses 1999/468/EG des Rates vom 28. Juni 1999 zur Festlegung der Modalitäten für die Ausübung der der Kommission übertragenen Durchführungsbefugnisse [1] zu erlassen.

(27) Die Kommission nimmt zwei Jahre nach der Umsetzung dieser Richtlinie eine Überprüfung vor, um unter anderem sicherzustellen, daß der technologische Fortschritt oder Änderungen des rechtlichen Umfelds keine Hindernisse für die Realisierung der erklärten Ziele dieser Richtlinie mit sich gebracht haben. Sie sollte die Auswirkungen verwandter technischer Bereiche prüfen und dem Europäischen Parlament und dem Rat hierüber einen Bericht vorlegen.

(28) Nach den in Artikel 5 des Vertrags niedergelegten Grundsätzen der Subsidiarität und der Verhältnismäßigkeit kann das Ziel der Schaffung harmonisierter rechtlicher Rahmenbedingungen für die Bereitstellung elektronischer Signaturen und entsprechender Dienste von den Mitgliedstaaten nicht ausreichend erreicht werden und läßt sich daher besser durch die Gemeinschaft verwirklichen. Diese Richtlinie geht nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Anwendungsbereich

Diese Richtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist.

Es werden weder Aspekte im Zusammenhang mit dem Abschluß und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen, für die nach einzelstaatlichem Recht oder Gemeinschaftsrecht Formvorschriften zu erfüllen sind, erfaßt, noch werden im einzelstaatlichen Recht oder im Gemeinschaftsrecht vorgesehene Regeln und Beschränkungen für die Verwendung von Dokumenten berührt.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

1. „elektronische Signatur“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen;
2. „fortgeschrittene elektronische Signatur“ eine elektronische Signatur, die folgende Anforderungen erfüllt:
   a) Sie ist ausschließlich dem Unterzeichner zugeordnet;
   b) sie ermöglicht die Identifizierung des Unterzeichners;
   c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
   d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, daß eine nachträgliche Veränderung der Daten erkannt werden kann;
3. „Unterzeichner“ eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt;
4. „Signaturerstellungsdaten“ einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden;
5. „Signaturerstellungseinheit“ eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird;
6. „sichere Signaturerstellungseinheit“ eine Signaturerstellungseinheit, die die Anforderungen des Anhangs III erfüllt;
7. „Signaturprüfdaten“ Daten wie Codes oder öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;
8. „Signaturprüfeinheit“ eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturprüfdaten verwendet wird;
9. „Zertifikat“ eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird;
10. „qualifiziertes Zertifikat“ ein Zertifikat, das die Anforderungen des Anhangs I erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des Anhangs II erfüllt;
11. „Zertifizierungsdiensteanbieter“ eine Stelle oder eine juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt;
12. „Produkt für elektronische Signaturen“ Hard- oder Software bzw. deren spezifische Komponenten, die von einem Zertifizierungsdiensteanbieter für die Bereitstellung von Diensten für elektronische Signaturen verwendet werden sollen oder die für die Erstellung und Überprüfung elektronischer Signaturen verwendet werden sollen;
13. „freiwillige Akkreditierung“ eine Erlaubnis, mit der die Rechte und Pflichten für die Erbringung von Zertifizierungsdiensten festgelegt werden und die auf Antrag des betreffenden Zertifizierungsdiensteanbieters von der öffentlichen oder privaten Stelle, die für die Festlegung dieser Rechte und Pflichten sowie für die Überwachung ihrer Einhaltung zuständig ist, erteilt wird, wenn der Zertifizierungsdiensteanbieter die sich aus der Erlaubnis ergebenden Rechte nicht ausüben darf, bevor er den Bescheid der Stelle erhalten hat.

[1] ABl. L 184 vom 17.7.1999, S. 23.

Artikel 3

Marktzugang

(1) Die Mitgliedstaaten machen die Bereitstellung von Zertifizierungsdiensten nicht von einer vorherigen Genehmigung abhängig.

(2) Unbeschadet des Absatzes 1 können die Mitgliedstaaten freiwillige Akkreditierungssysteme einführen bzw. beibehalten, die auf die Steigerung des Niveaus der erbrachten Zertifizierungsdienste abzielen. Alle mit diesen Systemen verknüpften Anforderungen müssen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein. Die Mitgliedstaaten dürfen die Zahl der akkreditierten Zertifizierungsdiensteanbieter nicht aus Gründen einschränken, die in den Geltungsbereich dieser Richtlinie fallen.

(3) Die Mitgliedstaaten tragen dafür Sorge, daß ein geeignetes System zur Überwachung der in ihrem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter, die öffentlich qualifizierte Zertifikate ausstellen, eingerichtet wird.

(4) Die Übereinstimmung sicherer Signaturerstellungseinheiten mit den Anforderungen nach Anhang III wird von geeigneten öffentlichen oder privaten Stellen festgestellt, die von den Mitgliedstaaten benannt werden. Die Kommission legt nach dem Verfahren des Artikels 9 Kriterien fest, anhand deren die Mitgliedstaaten bestimmen, ob eine Stelle zur Benennung geeignet ist.

Die von den in Unterabsatz 1 genannten Stellen vorgenommene Feststellung der Übereinstimmung mit den Anforderungen des Anhangs III wird von allen Mitgliedstaaten anerkannt.

(5) Die Kommission kann nach dem Verfahren des Artikels 9 Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen festlegen und im *Amtsblatt der Europäischen Gemeinschaften* veröffentlichen. Die Mitgliedstaaten gehen davon aus, daß die Anforderungen nach Anhang II Buchstabe f) und Anhang III erfüllt sind, wenn ein Produkt für elektronische Signaturen diesen Normen entspricht.

(6) Die Mitgliedstaaten und die Kommission arbeiten unter Berücksichtigung der Empfehlungen für die sichere Signaturprüfung in Anhang IV und im Interesse des Verbrauchers zusammen, um die Entwicklung und die Nutzung von Signaturprüfeinheiten zu fördern.

(7) Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich möglichen zusätzlichen Anforderungen unterwerfen. Diese Anforderungen müssen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen. Diese Anforderungen dürfen für grenzüberschreitende Dienste für den Bürger kein Hindernis darstellen.

Artikel 4

Binnenmarktgrundsätze

(1) Jeder Mitgliedstaat wendet die innerstaatlichen Bestimmungen, die er aufgrund dieser Richtlinie erläßt, auf die in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter und deren Dienste an. Die Mitgliedstaaten dürfen die Bereitstellung von Zertifizierungsdiensten, die aus anderen Mitgliedstaaten stammen, in den unter diese Richtlinie fallenden Bereichen nicht einschränken.

(2) Die Mitgliedstaaten tragen dafür Sorge, daß Produkte für elektronische Signaturen, die den Anforderungen dieser Richtlinie entsprechen, frei im Binnenmarkt verkehren können.

Artikel 5

Rechtswirkung elektronischer Signaturen

(1) Die Mitgliedstaaten tragen dafür Sorge, daß fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,

a) die rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen, und

b) in Gerichtsverfahren als Beweismittel zugelassen sind.

(2) Die Mitgliedstaaten tragen dafür Sorge, daß einer elektronischen Signatur die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen wird,

— weil sie in elektronischer Form vorliegt oder

— nicht auf einem qualifizierten Zertifikat beruht oder

— nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder

— nicht von einer sicheren Signaturerstellungseinheit erstellt wurde.

Artikel 6

Haftung

(1) Die Mitgliedstaaten gewährleisten als Mindestregelung, daß ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausstellt oder für ein derartiges Zertifikat öffentlich einsteht, in bezug auf Schäden gegenüber einer Stelle oder einer juristischen oder natürlichen Person, die vernünftigerweise auf das Zertifikat vertraut, dafür haftet, daß

a) alle Informationen in dem qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung richtig sind und das Zertifikat alle für ein qualifiziertes Zertifikat vorgeschriebenen Angaben enthält,

b) der in dem qualifizierten Zertifikat angegebene Unterzeichner zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturerstellungsdaten war, die den im Zertifikat angegebenen bzw. identifizierten Signaturprüfdaten entsprechen,

c) in Fällen, in denen der Zertifizierungsdiensteanbieter sowohl die Signaturerstellungsdaten als auch die Signaturprüfdaten erzeugt, beide Komponenten in komplementärer Weise genutzt werden können,

es sei denn, der Zertifizierungsdiensteanbieter weist nach, daß er nicht fahrlässig gehandelt hat.

(2) Die Mitgliedstaaten gewährleisten als Mindestregelung, daß ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausgestellt hat, in bezug auf Schäden gegenüber einer Stelle oder einer juristischen oder natürlichen Person, die vernünftigerweise auf das Zertifikat vertraut, für den Fall haftet, daß der Widerruf des Zertifikats nicht registriert worden ist, es sei denn, der Zertifizierungsdiensteanbieter weist nach, daß er nicht fahrlässig gehandelt hat.

(3) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifizierungsdiensteanbieter in einem qualifizierten Zertifikat Beschränkungen für die Verwendung des Zertifikates angeben können; diese Beschränkungen müssen für Dritte erkennbar sein. Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus einer über diese Beschränkungen hinausgehenden Verwendung des qualifizierten Zertifikats ergeben.

(4) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifizierungsdiensteanbieter in dem qualifizierten Zertifikat eine Grenze für den Wert der Transaktionen angeben können, für die das Zertifikat verwendet werden kann; diese Grenze muß für Dritte erkennbar sein.

Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus der Überschreitung dieser Höchstgrenze ergeben.

(5) Die Absätze 1 bis 4 gelten unbeschadet der Richtlinie 93/13/EWG des Rates vom 5. April 1993 über mißbräuchliche Klauseln in Verbraucherverträgen [1].

Artikel 7

Internationale Aspekte

(1) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifikate, die von einem Zertifizierungsdiensteanbieter eines Drittlandes öffentlich als qualifizierte Zertifikate ausgestellt werden, den von einem in der Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellten Zertifikaten rechtlich gleichgestellt werden, wenn

a) der Zertifizierungsdiensteanbieter die Anforderungen dieser Richtlinie erfüllt und im Rahmen eines freiwilligen Akkreditierungssystems eines Mitgliedstaats akkreditiert ist oder

b) ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen dieser Richtlinie erfüllt, für das Zertifikat einsteht oder

c) das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Gemeinschaft und Drittländern oder internationalen Organisationen anerkannt ist.

(2) Um grenzüberschreitende Zertifizierungsdienste mit Drittländern und die rechtliche Anerkennung fortgeschrittener elektronischer Signaturen, die aus Drittländern stammen, zu erleichtern, unterbreitet die Kommission gegebenenfalls Vorschläge mit dem Ziel, die effiziente Umsetzung von Normen und internationalen Vereinbarungen über Zertifizierungsdienste zu erreichen. Insbesondere unterbreitet sie dem Rat bei Bedarf Vorschläge zur Erteilung von geeigneten Mandaten zur Aushandlung bilateraler und multilateraler Vereinbarungen mit Drittländern und internationalen Organisationen. Der Rat beschließt mit qualifizierter Mehrheit.

(3) Wird die Kommission über Schwierigkeiten unterrichtet, auf die Unternehmen der Gemeinschaft beim Marktzugang in Drittländern stoßen, so kann sie erforderlichenfalls dem Rat Vorschläge für ein geeignetes Mandat zur Aushandlung vergleichbarer Rechte für Unternehmen der Gemeinschaft in diesen Drittländern vorlegen. Der Rat beschließt mit qualifizierter Mehrheit.

Die gemäß diesem Absatz ergriffenen Maßnahmen lassen die Verpflichtungen der Gemeinschaft und der Mitgliedstaaten im Rahmen der einschlägigen internationalen Übereinkünfte unberührt.

Artikel 8

Datenschutz

(1) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifizierungsdiensteanbieter und die für die Akkreditierung und Aufsicht zuständigen nationalen Stellen die Anforderungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [2] erfüllen.

(2) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifizierungsdiensteanbieter, die öffentlich Zertifikate ausstellen, personenbezogene Daten nur unmittelbar von der betroffenen Person oder mit ausdrücklicher Zustimmung der betroffenen Person und nur insoweit einholen können, als dies zur Ausstellung und Aufrechterhaltung des Zertifikats erforderlich ist. Die Daten dürfen ohne ausdrückliche Zustimmung der betroffenen Person nicht für anderweitige Zwecke erfaßt oder verarbeitet werden.

(3) Unbeschadet der Rechtswirkungen, die Pseudonyme nach einzelstaatlichem Recht haben, hindern die Mitgliedstaaten Zertifizierungsdiensteanbieter nicht daran, im Zertifikat ein Pseudonym anstelle des Namens des Unterzeichners anzugeben.

Artikel 9

Ausschuß

(1) Die Kommission wird von einem „Ausschuß für elektronische Signaturen“ (im folgenden „Ausschuß“ genannt) unterstützt.

(2) Bei einer Bezugnahme auf diesen Absatz finden die Artikel 4 und 7 des Beschlusses 1999/468/EG Anwendung, wobei Artikel 8 desselben Beschlusses zu beachten ist.

Der Zeitraum nach Artikel 4 Absatz 3 des Beschlusses 1999/468/EG wird auf drei Monate festgesetzt.

(3) Der Ausschuß gibt sich eine Geschäftsordnung.

Artikel 10

Aufgaben des Ausschusses

Der Ausschuß präzisiert die in den Anhängen festgelegten Anforderungen, die Kriterien nach Artikel 3 Absatz 4 und die allgemein anerkannten Normen für Produkte für elektronische Signaturen, die gemäß Artikel 3 Absatz 5 festgelegt und veröffentlicht werden, nach dem Verfahren des Artikels 9 Absatz 2.

[1] ABl. L 95 vom 21.4.1993, S. 29.

[2] ABl. L 281 vom 23.11.1995, S. 31.

Artikel 11

Notifizierung

(1) Die Mitgliedstaaten übermitteln der Kommission und den übrigen Mitgliedstaaten folgende Informationen:

a) Angaben zu nationalen freiwilligen Akkreditierungssystemen einschließlich zusätzlicher Anforderungen gemäß Artikel 3 Absatz 7,

b) Namen und Anschriften der für Akkreditierung und Aufsicht zuständigen nationalen Stellen und der in Artikel 3 Absatz 4 genannten Stellen sowie

c) Namen und Anschriften aller akkreditierten nationalen Zertifizierungsdiensteanbieter.

(2) Die Informationen gemäß Absatz 1 und diesbezügliche Änderungen sind von den Mitgliedstaaten so bald wie möglich zu übermitteln.

Artikel 12

Überprüfung

(1) Die Kommission überprüft die Durchführung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat spätestens zum 19. Juli 2003 darüber Bericht.

(2) Bei der Überprüfung ist unter anderem festzustellen, ob der Anwendungsbereich dieser Richtlinie angesichts der technologischen und rechtlichen Entwicklungen und der Marktentwicklung geändert werden sollte. Der Bericht umfaßt insbesondere eine Bewertung der Harmonisierungsaspekte auf der Grundlage der gesammelten Erfahrungen. Gegebenenfalls sind dem Bericht Vorschläge für Rechtsvorschriften beizufügen.

Artikel 13

Durchführung

(1) Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie vor dem 19. Juli 2001 nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 14

Inkrafttreten

Diese Richtlinie tritt am Tag ihrer Veröffentlichung im *Amtsblatt der Europäischen Gemeinschaften* in Kraft.

Artikel 15

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am 13. Dezember 1999.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
N. FONTAINE	S. HASSI

ANHANG I

Anforderungen an qualifizierte Zertifikate

Qualifizierte Zertifikate müssen folgende Angaben enthalten:

a) Angabe, daß das Zertifikat als qualifiziertes Zertifikat ausgestellt wird;

b) Angabe des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist;

c) Name des Unterzeichners oder ein Pseudonym, das als solches zu identifizieren ist;

d) Platz für ein spezifisches Attribut des Unterzeichners, das gegebenenfalls je nach Bestimmungszweck des Zertifikats aufgenommen wird;

e) Signaturprüfdaten, die den vom Unterzeichner kontrollierten Signaturerstellungsdaten entsprechen;

f) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;

g) Identitätscode des Zertifikats;

h) die fortgeschrittene elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters;

i) gegebenenfalls Beschränkungen des Geltungsbereichs des Zertifikats und

j) gegebenenfalls Begrenzungen des Wertes der Transaktionen, für die das Zertifikat verwendet werden kann.

ANHANG II

Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen

Zertifizierungsdiensteanbieter

a) müssen die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten nachweisen;

b) müssen den Betrieb eines schnellen und sicheren Verzeichnisdienstes und eines sicheren und unverzüglichen Widerrufsdienstes gewährleisten;

c) müssen gewährleisten, daß Datum und Uhrzeit der Ausstellung oder des Widerrufs eines Zertifikats genau bestimmt werden können;

d) müssen mit geeigneten Mitteln nach einzelstaatlichem Recht die Identität und gegebenenfalls die spezifischen Attribute der Person überprüfen, für die ein qualifiziertes Zertifikat ausgestellt wird;

e) müssen Personal mit den für die angebotenen Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen; dazu gehören insbesondere Managementkompetenzen, Kenntnisse der Technologie elektronischer Signaturen und Vertrautheit mit angemessenen Sicherheitsverfahren; sie müssen ferner geeignete Verwaltungs- und Managementverfahren einhalten, die anerkannten Normen entsprechen;

f) müssen vertrauenswürdige Systeme und Produkte einsetzen, die vor Veränderungen geschützt sind und die die technische und kryptographische Sicherheit der von ihnen unterstützten Verfahren gewährleisten;

g) müssen Maßnahmen gegen Fälschungen von Zertifikaten ergreifen und in den Fällen, in denen sie Signaturerstellungsdaten erzeugen, die Vertraulichkeit während der Erzeugung dieser Daten gewährleisten;

h) müssen über ausreichende Finanzmittel verfügen, um den Anforderungen der Richtlinie entsprechend arbeiten zu können. Sie müssen insbesondere in der Lage sein, das Haftungsrisiko für Schäden zu tragen, zum Beispiel durch Abschluß einer entsprechenden Versicherung;

i) müssen alle einschlägigen Informationen über ein qualifiziertes Zertifikat über einen angemessenen Zeitraum aufzeichnen, um insbesondere für Gerichtsverfahren die Zertifizierung nachweisen zu können. Die Aufzeichnungen können in elektronischer Form erfolgen;

j) dürfen keine Signaturerstellungdaten von Personen speichern oder kopieren, denen Schlüsselmanagementdienste angeboten werden;

k) müssen, bevor sie in Vertragsbeziehungen mit einer Person eintreten, die von ihnen ein Zertifikat zur Unterstützung ihrer elektronischen Signatur wünscht, diese Person mit einem dauerhaften Kommunikationsmittel über die genauen Bedingungen für die Verwendung des Zertifikats informieren, wozu unter anderem Nutzungsbeschränkungen für das Zertifikat, die Existenz eines freiwilligen Akkreditierungssystems und das Vorgehen in Beschwerde- und Schlichtungsverfahren gehören. Diese Angaben müssen schriftlich — gegebenenfalls elektronisch übermittelt — in klar verständlicher Sprache vorliegen. Wichtige Teilinformationen werden auf Antrag auch Dritten zur Verfügung gestellt, die auf das Zertifikat vertrauen;

l) müssen vertrauenswürdige Systeme für die Speicherung von Zertifikaten in einer überprüfbaren Form verwenden, so daß

— nur befugte Personen Daten eingeben und ändern können;

— die Angaben auf ihre Echtheit hin überprüft werden können;

— Zertifikate nur in den Fällen öffentlich abrufbar sind, für die die Zustimmung des Inhabers des Zertifikats eingeholt wurde;

— technische Veränderungen, die die Einhaltung dieser Sicherheitsanforderungen beeinträchtigen, für den Betreiber klar ersichtlich sind.

ANHANG III

Anforderungen an sichere Signaturerstellungseinheiten

1. Sichere Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, daß
   a) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten praktisch nur einmal auftreten können und daß ihre Geheimhaltung hinreichend gewährleistet ist;
   b) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist;
   c) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten von dem rechtmäßigen Unterzeichner vor der Verwendung durch andere verläßlich geschützt werden können.
2. Sichere Signaturerstellungseinheiten verändern die zu unterzeichnenden Daten nicht und verhindern nicht, daß diese Daten dem Unterzeichner vor dem Signaturvorgang dargestellt werden.

ANHANG IV

Empfehlungen für die sichere Signaturprüfung

Während des Signaturprüfungsvorgangs ist mit hinreichender Sicherheit zu gewährleisten, daß

a) die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden,
b) die Signatur zuverlässig überprüft wird und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
c) der Überprüfer bei Bedarf den Inhalt der unterzeichneten Daten zuverlässig feststellen kann,
d) die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden,
e) das Ergebnis der Überprüfung sowie die Identität des Unterzeichners korrekt angezeigt werden,
f) die Verwendung eines Pseudonyms eindeutig angegeben wird, und
g) sicherheitsrelevante Veränderungen erkannt werden können.

Signaturgesetz

Im folgenden das Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (Signaturgesetz – SigG).

Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften

Vom 16. Mai 2001

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG)*)

Inhaltsübersicht

Erster Abschnitt

Allgemeine Bestimmungen

§ 1

Zweck und Anwendungsbereich

(1) Zweck des Gesetzes ist es, Rahmenbedingungen für elektronische Signaturen zu schaffen.

(2) Soweit nicht bestimmte elektronische Signaturen durch Rechtsvorschrift vorgeschrieben sind, ist ihre Verwendung freigestellt.

(3) Rechtsvorschriften können für die öffentlich-rechtliche Verwaltungstätigkeit bestimmen, dass der Einsatz qualifizierter elektronischer Signaturen zusätzlichen Anforderungen unterworfen wird. Diese Anforderungen müssen objektiv, verhältnismäßig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen.

§ 2

Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
2. „fortgeschrittene elektronische Signaturen“ elektronische Signaturen nach Nummer 1, die
   a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
   b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,

*) Die Mitteilungspflichten der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften (ABl. EG Nr. L 204 S. 37), zuletzt geändert durch die Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 (ABl. EG Nr. L 217 S. 18), sind beachtet worden.

c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und

d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,

3. „qualifizierte elektronische Signaturen“ elektronische Signaturen nach Nummer 2, die

a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und

b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,

4. „Signaturschlüssel“ einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,

5. „Signaturprüfschlüssel“ elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,

6. „Zertifikate“ elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird,

7. „qualifizierte Zertifikate“ elektronische Bescheinigungen nach Nummer 6 für natürliche Personen, die die Voraussetzungen des § 7 erfüllen und von Zertifizierungsdiensteanbietern ausgestellt werden, die mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen,

8. „Zertifizierungsdiensteanbieter“ natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen,

9. „Signaturschlüssel-Inhaber“ natürliche Personen, die Signaturschlüssel besitzen und denen die zugehörigen Signaturprüfschlüssel durch qualifizierte Zertifikate zugeordnet sind,

10. „sichere Signaturerstellungseinheiten“ Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen nach § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind,

11. „Signaturanwendungskomponenten“ Software- und Hardwareprodukte, die dazu bestimmt sind,

a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder

b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen,

12. „technische Komponenten für Zertifizierungsdienste“ Software- oder Hardwareprodukte, die dazu bestimmt sind,

a) Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen,

b) qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten oder

c) qualifizierte Zeitstempel zu erzeugen,

13. „Produkte für qualifizierte elektronische Signaturen“ sichere Signaturerstellungseinheiten, Signaturanwendungskomponenten und technische Komponenten für Zertifizierungsdienste,

14. „qualifizierte Zeitstempel“ elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllt, darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben,

15. „freiwillige Akkreditierung“ Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind.

§ 3

Zuständige Behörde

Die Aufgaben der zuständigen Behörde nach diesem Gesetz und der Rechtsverordnung nach § 24 obliegen der Behörde nach § 66 des Telekommunikationsgesetzes.

Zweiter Abschnitt

Zertifizierungsdiensteanbieter

§ 4

Allgemeine Anforderungen

(1) Der Betrieb eines Zertifizierungsdienstes ist im Rahmen der Gesetze genehmigungsfrei.

(2) Einen Zertifizierungsdienst darf nur betreiben, wer die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde sowie eine Deckungsvorsorge nach § 12 nachweist und die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 gewährleistet. Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Zertifizierungsdiensteanbieter die für den Betrieb maßgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb eines Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes liegen vor, wenn die Maßnahmen zur Erfüllung der Sicherheitsanforderungen nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 der zuständigen Behörde in einem Sicherheitskonzept aufgezeigt und geeignet und praktisch umgesetzt sind.

(3) Wer den Betrieb eines Zertifizierungsdienstes aufnimmt, hat dies der zuständigen Behörde spätestens mit der Betriebsaufnahme anzuzeigen. Mit der Anzeige ist in geeigneter Form darzulegen, dass die Voraussetzungen nach Absatz 2 vorliegen.

(4) Die Erfüllung der Voraussetzungen nach Absatz 2 ist über die gesamte Zeitdauer der Tätigkeit des Zertifizierungsdienstes sicherzustellen. Umstände, die dies nicht mehr ermöglichen, sind der zuständigen Behörde unverzüglich anzuzeigen.

(5) Der Zertifizierungsdiensteanbieter kann unter Einbeziehung in sein Sicherheitskonzept nach Absatz 2 Satz 4 Aufgaben nach diesem Gesetz und der Rechtsverordnung nach § 24 an Dritte übertragen.

§ 5

Vergabe von qualifizierten Zertifikaten

(1) Der Zertifizierungsdiensteanbieter hat Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren. Er hat die Zuordnung eines Signaturprüfschlüssels zu einer identifizierten Person durch ein qualifiziertes Zertifikat zu bestätigen und dieses jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten. Ein qualifiziertes Zertifikat darf nur mit Zustimmung des Signaturschlüssel-Inhabers abrufbar gehalten werden.

(2) Ein qualifiziertes Zertifikat kann auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie berufsbezogene oder sonstige Angaben zu seiner Person (Attribute) enthalten. Hinsichtlich der Angaben über die Vertretungsmacht ist die Einwilligung der dritten Person nachzuweisen; berufsbezogene oder sonstige Angaben zur Person sind durch die für die berufsbezogenen oder sonstigen Angaben zuständige Stelle zu bestätigen. Angaben über die Vertretungsmacht für eine dritte Person dürfen nur bei Nachweis der Einwilligung nach Satz 2, berufsbezogene oder sonstige Angaben des Antragstellers zur Person nur bei Vorlage der Bestätigung nach Satz 2 in ein qualifiziertes Zertifikat aufgenommen werden. Weitere personenbezogene Angaben dürfen in ein qualifiziertes Zertifikat nur mit Einwilligung des Betroffenen aufgenommen werden.

(3) Der Zertifizierungsdiensteanbieter hat auf Verlangen eines Antragstellers in einem qualifizierten Zertifikat an Stelle seines Namens ein Pseudonym aufzuführen. Enthält ein qualifiziertes Zertifikat Angaben über eine Vertretungsmacht für eine dritte Person oder berufsbezogene oder sonstige Angaben zur Person, ist eine Einwilligung der dritten Person oder der für die berufsbezogenen oder sonstigen Angaben zuständigen Stelle zur Verwendung des Pseudonyms erforderlich.

(4) Der Zertifzierungsdiensteanbieter hat Vorkehrungen zu treffen, damit Daten für qualifizierte Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Er hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten. Eine Speicherung von Signaturschlüsseln außerhalb der sicheren Signaturerstellungseinheit ist unzulässig.

(5) Der Zertifizierungsdiensteanbieter hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal und Produkte für qualifizierte elektronische Signaturen, die mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 dieses Gesetzes und der Rechtsverordnung nach § 24 erfüllen, einzusetzen.

(6) Der Zertifizierungsdiensteanbieter hat sich in geeigneter Weise zu überzeugen, dass der Antragsteller die zugehörige sichere Signaturerstellungseinheit besitzt.

§ 6

Unterrichtungspflicht

(1) Der Zertifizierungsdiensteanbieter hat den Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zur Sicherheit von qualifizierten elektronischen Signaturen und zu deren zuverlässiger Prüfung beizutragen. Er hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

(2) Der Zertifizierungsdiensteanbieter hat den Antragsteller darüber zu unterrichten, dass eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung hat wie eine eigenhändige Unterschrift, wenn durch Gesetz nicht ein anderes bestimmt ist.

(3) Zur Unterrichtung nach Absatz 1 und 2 ist dem Antragsteller eine schriftliche Belehrung auszuhändigen, deren Kenntnisnahme dieser durch gesonderte Unterschrift zu bestätigen hat. Soweit ein Antragsteller bereits zu einem früheren Zeitpunkt nach den Absätzen 1 und 2 unterrichtet worden ist, kann eine erneute Unterrichtung unterbleiben.

§ 7

Inhalt von qualifizierten Zertifikaten

(1) Ein qualifiziertes Zertifikat muss folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen:

1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muss,
2. den zugeordneten Signaturprüfschlüssel,
3. die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
4. die laufende Nummer des Zertifikates,
5. Beginn und Ende der Gültigkeit des Zertifikates,
6. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
7. Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist,
8. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
9. nach Bedarf Attribute des Signaturschlüssel-Inhabers.

(2) Attribute können auch in ein gesondertes qualifiziertes Zertifikat (qualifiziertes Attribut-Zertifikat) aufgenommen werden. Bei einem qualifizierten Attribut-Zertifikat können die Angaben nach Absatz 1 durch eindeutige Referenzdaten des qualifizierten Zertifikates, auf das sie Bezug nehmen, ersetzt werden, soweit sie nicht für die Nutzung des qualifizierten Attribut-Zertifikates benötigt werden.

§ 8

Sperrung von qualifizierten Zertifikaten

(1) Der Zertifizierungsdiensteanbieter hat ein qualifiziertes Zertifikat unverzüglich zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangt, das Zer-

tifikat auf Grund falscher Angaben zu § 7 ausgestellt wurde, der Zertifizierungsdiensteanbieter seine Tätigkeit beendet und diese nicht von einem anderen Zertifizierungsdiensteanbieter fortgeführt wird oder die zuständige Behörde gemäß § 19 Abs. 4 eine Sperrung anordnet. Die Sperrung muss den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig. Wurde ein qualifiziertes Zertifikat mit falschen Angaben ausgestellt, kann der Zertifizierungsdiensteanbieter dies zusätzlich kenntlich machen.

(2) Enthält ein qualifiziertes Zertifikat Angaben nach § 5 Abs. 2, so kann auch die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle, wenn die Voraussetzungen für die berufsbezogenen oder sonstigen Angaben zur Person nach Aufnahme in das qualifizierte Zertifikat entfallen, eine Sperrung des betreffenden Zertifikates nach Absatz 1 verlangen.

§ 9

Qualifizierte Zeitstempel

Stellt ein Zertifizierungsdiensteanbieter qualifizierte Zeitstempel aus, so gilt § 5 Abs. 5 entsprechend.

§ 10

Dokumentation

(1) Der Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 sowie die ausgestellten qualifizierten Zertifikate nach Maßgabe des Satzes 2 so zu dokumentieren, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Die Dokumentation muss unverzüglich so erfolgen, dass sie nachträglich nicht unbemerkt verändert werden kann. Dies gilt insbesondere für die Ausstellung und Sperrung von qualifizierten Zertifikaten.

(2) Dem Signaturschlüssel-Inhaber ist auf Verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte zu gewähren.

§ 11

Haftung

(1) Verletzt ein Zertifizierungsdiensteanbieter die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 oder versagen seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen, so hat er einem Dritten den Schaden zu ersetzen, den dieser dadurch erleidet, dass er auf die Angaben in einem qualifizierten Zertifikat, einem qualifizierten Zeitstempel oder einer Auskunft nach § 5 Abs. 1 Satz 2 vertraut. Die Ersatzpflicht tritt nicht ein, wenn der Dritte die Fehlerhaftigkeit der Angabe kannte oder kennen musste.

(2) Die Ersatzpflicht tritt nicht ein, wenn der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt hat.

(3) Wenn ein qualifiziertes Zertifikat die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt, tritt die Ersatzpflicht nur im Rahmen dieser Beschränkungen ein.

(4) Der Zertifizierungsdiensteanbieter haftet für beauftragte Dritte nach § 4 Abs. 5 und beim Einstehen für ausländische Zertifikate nach § 23 Abs. 1 Nr. 2 wie für eigenes Handeln. § 831 Abs. 1 Satz 2 des Bürgerlichen Gesetzbuchs findet keine Anwendung.

§ 12

Deckungsvorsorge

Der Zertifizierungsdiensteanbieter ist verpflichtet, eine geeignete Deckungsvorsorge zu treffen, damit er seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachkommen kann, die dadurch entstehen, dass er die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 verletzt oder seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen versagen. Die Mindestsumme beträgt jeweils 500 000 Deutsche Mark für einen durch ein haftungsauslösendes Ereignis der in Satz 1 bezeichneten Art verursachten Schaden.

§ 13

Einstellung der Tätigkeit

(1) Der Zertifizierungsdiensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der zuständigen Behörde anzuzeigen. Er hat dafür zu sorgen, dass die bei Einstellung der Tätigkeit gültigen qualifizierten Zertifikate von einem anderen Zertifizierungsdiensteanbieter übernommen werden, oder diese zu sperren. Er hat die betroffenen Signaturschlüssel-Inhaber über die Einstellung seiner Tätigkeit und die Übernahme der qualifizierten Zertifikate durch einen anderen Zertifizierungsdiensteanbieter zu benachrichtigen.

(2) Der Zertifizierungsdiensteanbieter hat die Dokumentation nach § 10 an den Zertifizierungsdiensteanbieter, welcher die Zertifikate nach Absatz 1 übernimmt, zu übergeben. Übernimmt kein anderer Zertifizierungsdiensteanbieter die Dokumentation, so hat die zuständige Behörde diese zu übernehmen. Die zuständige Behörde erteilt bei Vorliegen eines berechtigten Interesses Auskunft zur Dokumentation nach Satz 2, soweit dies technisch ohne unverhältnismäßig großen Aufwand möglich ist.

(3) Der Zertifizierungsdiensteanbieter hat einen Antrag auf Eröffnung eines Insolvenzverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

§ 14

Datenschutz

(1) Der Zertifizierungsdiensteanbieter darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines qualifizierten Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz es erlaubt oder der Betroffene eingewilligt hat.

(2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat der Zertifizierungsdiensteanbieter die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist oder

soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen. Die Auskünfte sind zu dokumentieren. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber über die Aufdeckung des Pseudonyms zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüssel-Inhabers an der Unterrichtung überwiegt.

(3) Soweit andere als die in § 2 Nr. 8 genannten Zertifizierungsdiensteanbieter Zertifikate für elektronische Signaturen ausstellen, gelten die Absätze 1 und 2 entsprechend.

Dritter Abschnitt

Freiwillige Akkreditierung

§ 15

Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern

(1) Zertifizierungsdiensteanbieter können sich auf Antrag von der zuständigen Behörde akkreditieren lassen; die zuständige Behörde kann sich bei der Akkreditierung privater Stellen bedienen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 erfüllt sind. Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen der zuständigen Behörde. Mit diesem wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen (qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung) zum Ausdruck gebracht. Sie dürfen sich als akkreditierte Zertifizierungsdiensteanbieter bezeichnen und sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen.

(2) Zur Erfüllung der Voraussetzungen nach Absatz 1 muss das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 durch eine Stelle nach § 18 umfassend auf seine Eignung und praktische Umsetzung geprüft und bestätigt sein. Die Prüfung und Bestätigung ist nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen.

(3) Die Akkreditierung kann mit Nebenbestimmungen versehen werden, soweit dies erforderlich ist, um die Erfüllung der Voraussetzungen nach diesem Gesetz und der Rechtsverordnung nach § 24 bei Aufnahme und während des Betriebes sicherzustellen.

(4) Die Akkreditierung ist zu versagen, wenn die Voraussetzungen nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt sind; § 19 findet entsprechend Anwendung.

(5) Bei Nichterfüllung der Pflichten aus diesem Gesetz oder der Rechtsverordnung nach § 24 oder bei Vorliegen eines Versagungsgrundes nach Absatz 4 hat die zuständige Behörde die Akkreditierung zu widerrufen oder diese, soweit die Gründe bereits zum Zeitpunkt der Akkreditierung vorlagen, zurückzunehmen, wenn Maßnahmen nach § 19 Abs. 2 keinen Erfolg versprechen.

(6) Im Falle des Widerrufs oder der Rücknahme einer Akkreditierung oder im Falle der Einstellung der Tätigkeit eines akkreditierten Zertifizierungsdiensteanbieters hat die zuständige Behörde eine Übernahme der Tätigkeit durch einen anderen akkreditierten Zertifizierungsdiensteanbieter oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen. Dies gilt auch bei Antrag auf Eröffnung eines Insolvenzverfahrens, wenn die Tätigkeit nicht fortgesetzt wird. Übernimmt kein anderer akkreditierter Zertifizierungsdiensteanbieter die Dokumentation gemäß § 13 Abs. 2, so hat die zuständige Behörde diese zu übernehmen; § 10 Abs. 1 Satz 1 gilt entsprechend.

(7) Bei Produkten für qualifizierte elektronische Signaturen muss die Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 und der Rechtsverordnung nach § 24 nach dem Stand von Wissenschaft und Technik hinreichend geprüft und durch eine Stelle nach § 18 bestätigt worden sein; Absatz 1 Satz 3 findet entsprechende Anwendung. Der akkreditierte Zertifizierungsdiensteanbieter hat

1. für seine Zertifizierungstätigkeit nur nach Satz 1 geprüfte und bestätigte Produkte für qualifizierte elektronische Signaturen einzusetzen,
2. qualifizierte Zertifikate nur für Personen auszustellen, die nachweislich nach Satz 1 geprüfte und bestätigte sichere Signaturerstellungseinheiten besitzen, und
3. die Signaturschlüssel-Inhaber im Rahmen des § 6 Abs. 1 über nach Satz 1 geprüfte und bestätigte Signaturanwendungskomponenten zu unterrichten.

§ 16

Zertifikate der zuständigen Behörde

(1) Die zuständige Behörde stellt den akkreditierten Zertifizierungsdiensteanbietern die für ihre Tätigkeit benötigten qualifizierten Zertifikate aus. Die Vorschriften für die Vergabe von qualifizierten Zertifikaten durch akkreditierte Zertifizierungsdiensteanbieter gelten für die zuständige Behörde entsprechend. Sie sperrt von ihr ausgestellte qualifizierte Zertifikate, wenn ein akkreditierter Zertifizierungsdiensteanbieter seine Tätigkeit einstellt oder wenn eine Akkreditierung zurückgenommen oder widerrufen wird.

(2) Die zuständige Behörde hat

1. die Namen, Anschriften und Kommunikationsverbindungen der akkreditierten Zertifizierungsdiensteanbieter,
2. den Widerruf oder die Rücknahme einer Akkreditierung,
3. die von ihr ausgestellten qualifizierten Zertifikate und deren Sperrung und
4. die Beendigung und die Untersagung des Betriebes eines akkreditierten Zertifizierungsdiensteanbieters

jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten.

(3) Bei Bedarf stellt die zuständige Behörde auch die von den Zertifizierungsdiensteanbietern oder Herstellern benötigten elektronischen Bescheinigungen für die automatische Authentifizierung von Produkten nach § 15 Abs. 7 aus.

Vierter Abschnitt

Technische Sicherheit

§ 17

Produkte für qualifizierte elektronische Signaturen

(1) Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. Werden die Signaturschlüssel auf einer sicheren Signaturerstellungseinheit selbst erzeugt, so gilt Absatz 3 Nr. 1 entsprechend.

(2) Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht. Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

1. auf welche Daten sich die Signatur bezieht,
2. ob die signierten Daten unverändert sind,
3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und
5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat.

Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.

(3) Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um

1. bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen,
2. qualifizierte Zertifikate, die gemäß § 5 Abs. 1 Satz 2 nachprüfbar oder abrufbar gehalten werden, vor unbefugter Veränderung und unbefugtem Abruf zu schützen sowie
3. bei Erzeugung qualifizierter Zeitstempel Fälschungen und Verfälschungen auszuschließen.

(4) Die Erfüllung der Anforderungen nach den Absätzen 1 und 3 Nr. 1 sowie der Rechtsverordnung nach § 24 ist durch eine Stelle nach § 18 zu bestätigen. Zur Erfüllung der Anforderungen nach den Absätzen 2 und 3 Nr. 2 und 3 genügt eine Erklärung durch den Hersteller des Produkts für qualifizierte elektronische Signaturen.

§ 18

Anerkennung von Prüf- und Bestätigungsstellen

(1) Die zuständige Behörde erkennt eine natürliche oder juristische Person auf Antrag als Bestätigungsstelle nach § 17 Abs. 4 oder § 15 Abs. 7 Satz 1 oder als Prüf- und Bestätigungsstelle nach § 15 Abs. 2 an, wenn diese die für die Tätigkeit erforderliche Zuverlässigkeit, Unabhängigkeit und Fachkunde nachweist. Die Anerkennung kann inhaltlich beschränkt, vorläufig oder mit einer Befristung versehen erteilt werden und mit Auflagen verbunden sein.

(2) Die nach Absatz 1 anerkannten Stellen haben ihre Aufgaben unparteiisch, weisungsfrei und gewissenhaft zu erfüllen. Sie haben die Prüfungen und Bestätigungen zu dokumentieren und die Dokumentation im Falle der Einstellung ihrer Tätigkeit an die zuständige Behörde zu übergeben.

Fünfter Abschnitt

Aufsicht

§ 19

Aufsichtsmaßnahmen

(1) Die Aufsicht über die Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 obliegt der zuständigen Behörde; diese kann sich bei der Durchführung der Aufsicht privater Stellen bedienen. Mit der Aufnahme des Betriebes unterliegt ein Zertifizierungsdiensteanbieter der Aufsicht der zuständigen Behörde.

(2) Die zuständige Behörde kann gegenüber Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 treffen.

(3) Die zuständige Behörde hat einem Zertifizierungsdiensteanbieter den Betrieb vorübergehend, teilweise oder ganz zu untersagen, wenn Tatsachen die Annahme rechtfertigen, dass er

1. nicht die für den Betrieb eines Zertifizierungsdienstes erforderliche Zuverlässigkeit besitzt,
2. nicht nachweist, dass die für den Betrieb erforderliche Fachkunde vorliegt,
3. nicht über die erforderliche Deckungsvorsorge verfügt,
4. ungeeignete Produkte für qualifizierte elektronische Signaturen verwendet oder
5. die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt

und Maßnahmen nach Absatz 2 keinen Erfolg versprechen.

(4) Die zuständige Behörde kann eine Sperrung von qualifizierten Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, dass qualifizierte Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder dass sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung qualifizierter elektronischer Signaturen oder eine unbemerkte Verfälschung damit signierter Daten zulassen.

(5) Die Gültigkeit der von einem Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikate bleibt von

der Untersagung des Betriebes und der Einstellung der Tätigkeit sowie der Rücknahme und dem Widerruf einer Akkreditierung unberührt.

(6) Die zuständige Behörde hat die Namen der bei ihr angezeigten Zertifizierungsdiensteanbieter sowie der Zertifizierungsdiensteanbieter, die ihre Tätigkeit nach § 13 eingestellt haben oder deren Betrieb nach § 19 Abs. 3 untersagt wurde, für jeden über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten.

§ 20

Mitwirkungspflicht

(1) Die Zertifizierungsdiensteanbieter und die für diese nach § 4 Abs. 5 tätigen Dritten haben der zuständigen Behörde und den in ihrem Auftrag handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen in geeigneter Weise zur Einsicht vorzulegen, auch soweit sie in elektronischer Form geführt werden, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren.

(2) Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft verweigern, wenn er sich damit selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Er ist auf dieses Recht hinzuweisen.

Sechster Abschnitt

Schlussbestimmungen

§ 21

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4 Abs. 2 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, 3 und 4, einen Zertifizierungsdienst betreibt,
2. entgegen § 4 Abs. 3 Satz 1 oder § 13 Abs. 1 Satz 1 eine Anzeige nicht, nicht richtig oder nicht rechtzeitig erstattet,
3. entgegen § 5 Abs. 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 eine Person nicht, nicht richtig oder nicht rechtzeitig identifiziert,
4. entgegen § 5 Abs. 1 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, ein qualifiziertes Zertifikat nicht nachprüfbar hält,
5. entgegen § 5 Abs. 1 Satz 3 ein qualifiziertes Zertifikat abrufbar hält,
6. entgegen § 5 Abs. 2 Satz 3 oder 4 eine Angabe in ein qualifiziertes Zertifikat aufnimmt,
7. entgegen § 5 Abs. 4 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, eine Vorkehrung nicht oder nicht richtig trifft,
8. entgegen § 5 Abs. 4 Satz 3 einen Signaturschlüssel speichert,
9. entgegen § 10 Abs. 1 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, eine Sicherheitsmaßnahme oder ein qualifiziertes Zertifikat nicht, nicht richtig oder nicht rechtzeitig dokumentiert,
10. entgegen § 13 Abs. 1 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, nicht dafür sorgt, dass ein qualifiziertes Zertifikat von einem anderen Zertifizierungsdiensteanbieter übernommen wird und ein qualifiziertes Zertifikat nicht oder nicht rechtzeitig sperrt oder
11. entgegen § 13 Abs. 1 Satz 3 in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 einen Signaturschlüssel-Inhaber nicht, nicht richtig oder nicht rechtzeitig benachrichtigt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 1, 7 und 8 mit einer Geldbuße bis zu hunderttausend Deutsche Mark, in den übrigen Fällen mit einer Geldbuße bis zu zwanzigtausend Deutsche Mark geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Regulierungsbehörde für Telekommunikation und Post.

§ 22

Kosten und Beiträge

(1) Die zuständige Behörde erhebt für ihre folgenden Amtshandlungen Kosten (Gebühren und Auslagen):

1. Maßnahmen im Rahmen der freiwilligen Akkreditierung von Zertifizierungsdiensteanbietern nach § 15 und der Rechtsverordnung nach § 24,
2. Maßnahmen im Rahmen der Ausstellung der qualifizierten Zertifikate nach § 16 Abs. 1 sowie der Ausstellung von Bescheinigungen nach § 16 Abs. 3,
3. Maßnahmen im Rahmen der Anerkennung von Prüf- und Bestätigungsstellen nach § 18 und der Rechtsverordnung nach § 24,
4. Maßnahmen im Rahmen der Aufsicht nach § 19 Abs. 1 bis 4 in Verbindung mit § 4 Abs. 2 bis 4 und der Rechtsverordnung nach § 24.

Kosten werden auch für den Verwaltungsaufwand erhoben, der dadurch entsteht, dass sich die Behörde bei der Durchführung der Aufsicht privater Stellen bedient. Das Verwaltungskostengesetz findet Anwendung.

(2) Zertifizierungsdiensteanbieter, die den Betrieb nach § 4 Abs. 3 angezeigt haben, haben zur Abgeltung des Verwaltungsaufwands für die ständige Erfüllung der Voraussetzungen nach § 19 Abs. 6 eine Abgabe an die zuständige Behörde zu entrichten, die als Jahresbeitrag erhoben wird. Zertifizierungsdiensteanbieter, die nach § 15 Abs. 1 akkreditiert sind, haben zur Abgeltung des Verwaltungsaufwands für die ständige Erfüllung der Voraussetzungen nach § 16 Abs. 2 eine Abgabe an die zuständige Behörde zu entrichten, die als Jahresbeitrag erhoben wird.

§ 23

Ausländische elektronische Signaturen und Produkte für elektronische Signaturen

(1) Elektronische Signaturen, für die ein ausländisches qualifiziertes Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Ver-

tragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie Artikel 5 Abs. 1 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000 Nr. L 13 S. 2) in der jeweils geltenden Fassung entsprechen, qualifizierten elektronischen Signaturen gleichgestellt. Elektronische Signaturen aus Drittstaaten sind qualifizierten elektronischen Signaturen gleichgestellt, wenn das Zertifikat von einem dortigen Zertifizierungsdiensteanbieter öffentlich als qualifiziertes Zertifikat ausgestellt und für eine elektronische Signatur im Sinne von Artikel 5 Abs. 1 der Richtlinie 1999/93/EG bestimmt ist und wenn

1. der Zertifizierungsdiensteanbieter die Anforderungen der Richtlinie erfüllt und in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum akkreditiert ist oder
2. ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, welcher die Anforderungen der Richtlinie erfüllt, für das Zertifikat einsteht oder
3. das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Union und Drittstaaten oder internationalen Organisationen anerkannt ist.

(2) Elektronische Signaturen nach Absatz 1 sind qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung nach § 15 Abs. 1 gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.

(3) Produkte für elektronische Signaturen, bei denen in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum festgestellt wurde, dass sie den Anforderungen der Richtlinie 1999/93/EG in der jeweils geltenden Fassung entsprechen, werden anerkannt. Den nach § 15 Abs. 7 geprüften Produkten für qualifizierte elektronische Signaturen werden Produkte für elektronische Signaturen aus einem in Satz 1 genannten Staat oder aus einem Drittstaat gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.

§ 24

Rechtsverordnung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die zur Durchführung der §§ 3 bis 23 erforderlichen Rechtsvorschriften zu erlassen über

1. die Ausgestaltung der Pflichten der Zertifizierungsdiensteanbieter in Bezug auf die Betriebsaufnahme und während des Betriebes sowie bei Einstellung des Betriebes nach § 4 Abs. 2 und 3, §§ 5, 6 Abs. 1, §§ 8, 10, 13 und 15,
2. die gebührenpflichtigen Tatbestände und die Gebührensätze sowie die Höhe der Beiträge und das Verfahren der Beitragserhebung durch die zuständige Behörde; bei der Bemessung der Beiträge ist der Verwaltungsaufwand (Personal- und Sachaufwand) sowie Investitionsaufwand zugrunde zu legen soweit er nicht bereits durch eine Gebühr abgegolten wird,
3. die Ausgestaltung des Inhalts und die Gültigkeitsdauer von qualifizierten Zertifikaten nach § 7,
4. die zur Erfüllung der Verpflichtung zur Deckungsvorsorge nach § 12 zulässigen Sicherheitsleistungen sowie deren Umfang, Höhe und inhaltliche Ausgestaltung,
5. die näheren Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 1 bis 3 sowie die Prüfung dieser Produkte und die Bestätigung, dass die Anforderungen erfüllt sind, nach § 17 Abs. 4 und § 15 Abs. 7,
6. die Einzelheiten des Verfahrens der Anerkennung sowie der Tätigkeit von Prüf- und Bestätigungsstellen nach § 18,
7. den Zeitraum sowie das Verfahren, nach dem Daten mit einer qualifizierten elektronischen Signatur nach § 6 Abs. 1 Satz 2 neu signiert werden sollten,
8. das Verfahren zur Feststellung der gleichwertigen Sicherheit von ausländischen elektronischen Signaturen und ausländischen Produkten für elektronische Signaturen nach § 23.

§ 25

Übergangsvorschriften

(1) Die nach dem Signaturgesetz vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), genehmigten Zertifizierungsstellen gelten als akkreditiert im Sinne von § 15. Diese haben der zuständigen Behörde innerhalb von drei Monaten nach Inkrafttreten dieses Gesetzes einen Deckungsnachweis nach § 12 vorzulegen.

(2) Die von den Zertifizierungsstellen nach Absatz 1 bis zum Zeitpunkt des Inkrafttretens dieses Gesetzes nach § 5 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), ausgestellten Zertifikate sind qualifizierten Zertifikaten gleichgestellt. Inhaber von Zertifikaten nach Satz 1 sind innerhalb von sechs Monaten nach Inkrafttreten dieses Gesetzes durch die Zertifizierungsstelle nach § 6 Abs. 2 in geeigneter Weise zu unterrichten.

(3) Die von der zuständigen Behörde erfolgten Anerkennungen von Prüf- und Bestätigungsstellen nach § 4 Abs. 3 Satz 3 und § 14 Abs. 4 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), behalten ihre Gültigkeit, soweit sie in Übereinstimmung mit § 18 dieses Gesetzes stehen.

(4) Technische Komponenten, bei denen die Erfüllung der Anforderungen nach § 14 Abs. 4 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872) geprüft und bestätigt wurde, sind Produkten für qualifizierte elektronische Signaturen nach § 15 Abs. 7 dieses Gesetzes gleichgestellt.

Artikel 2

Umstellung von Vorschriften auf Euro

Das Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876) wird wie folgt geändert:

1. In § 12 Satz 2 wird die Angabe „500 000 Deutsche Mark“ durch die Angabe „250 000 Euro“ ersetzt.
2. In § 21 Abs. 2 werden die Wörter „hunderttausend Deutsche Mark“ durch die Wörter „fünfzigtausend

Euro“ und die Wörter „zwanzigtausend Deutsche Mark“ durch die Wörter „zehntausend Euro“ ersetzt.

Artikel 3

Anpassung von Bundesrecht

(1) In § 15 Satz 2 der Verordnung über die Vergabe öffentlicher Aufträge vom 9. Januar 2001 (BGBl. I S. 110) werden die Wörter „Signatur im Sinne des Signaturgesetzes“ durch die Wörter „einer qualifizierten elektronischen Signatur nach dem Signaturgesetz“ ersetzt.

(2) In § 7 Abs. 3 der Sozialversicherungs-Rechnungsverordnung vom 15. Juli 1999 (BGBl. I S. 1627) wird die Angabe „digitalen Signatur nach § 2 Abs. 1 des Signaturgesetzes (Artikel 3 des Gesetzes vom 22. Juli 1997, BGBl. I S. 1870, 1872)“ durch die Wörter „einer qualifizierten elektronischen Signatur nach dem Signaturgesetz“ ersetzt.

Artikel 4

Rückkehr zum einheitlichen Verordnungsrang

Die auf Artikel 3 Abs. 1 und 2 beruhenden Teile der dort geänderten Rechtsverordnung können auf Grund der jeweils einschlägigen Ermächtigungen durch Rechtsverordnung geändert werden.

Artikel 5

Inkrafttreten; Außerkrafttreten

Dieses Gesetz tritt vorbehaltlich des Satzes 2 am Tage nach der Verkündung in Kraft; gleichzeitig tritt das Signaturgesetz vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), außer Kraft. Artikel 2 tritt am 1. Januar 2002 in Kraft.

Die verfassungsmäßigen Rechte des Bundesrates sind gewahrt.

Das vorstehende Gesetz wird hiermit ausgefertigt und wird im Bundesgesetzblatt verkündet.

Berlin, den 16. Mai 2001

Der Bundespräsident
Johannes Rau

Der Bundeskanzler
Gerhard Schröder

Der Bundesminister
für Wirtschaft und Technologie
Müller

Signaturverordnung

Im folgenden die Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001.

Verordnung zur elektronischen Signatur (Signaturverordnung – SigV)*)

Vom 16. November 2001

Auf Grund des § 24 des Signaturgesetzes vom 16. Mai 2001 (BGBl. I S. 876) in Verbindung mit dem 2. Abschnitt des Verwaltungskostengesetzes vom 23. Juni 1970 (BGBl. I S. 821) verordnet die Bundesregierung:

Inhaltsübersicht

§ 1

Form, Inhalt und Änderung der Anzeige

(1) Eine Anzeige nach § 4 Abs. 3 des Signaturgesetzes ist schriftlich oder mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen bei der zuständigen Behörde vorzunehmen.

(2) Die Anzeige muss folgende Angaben und Unterlagen umfassen:

1. den Namen und die Anschrift des Zertifizierungsdiensteanbieters,
2. die Namen der gesetzlichen Vertreter,
3. aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für den Zertifizierungsdiensteanbieter und seine gesetzlichen Vertreter,
4. einen aktuellen Handelsregisterauszug oder eine vergleichbare Unterlage,

*) Die Mitteilungspflichten der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften (ABl. EG Nr. L 204 S. 37), zuletzt geändert durch die Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 (ABl. EG Nr. L 217 S. 18) sind beachtet worden.

5. Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde nach § 4 Abs. 2 Satz 3 des Signaturgesetzes,
6. ein Sicherheitskonzept mit einer genauen Darlegung, wie dieses umgesetzt ist, einschließlich der Übertragung von Aufgaben an Dritte nach § 4 Abs. 5 des Signaturgesetzes, und
7. einen Nachweis der Deckungsvorsorge nach § 12 des Signaturgesetzes.

Ändern sich die Umstände nach Satz 1 Nr. 1 oder Nr. 2 oder sicherheitserhebliche Umstände nach Satz 1 Nr. 6, ist die zuständige Behörde schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu informieren. § 2 bleibt unberührt.

(3) Soweit Teile des Zertifizierungsdienstes in einem Staat nach § 23 Abs. 1 Satz 1 des Signaturgesetzes oder unter den Bedingungen des § 23 Abs. 1 Satz 2 Nr. 3 des Signaturgesetzes in einem Drittstaat betrieben werden, sind zusätzlich Nachweise darüber vorzulegen, dass der Betrieb einer gleichwertigen Aufsicht unterliegt. Der Betrieb von Teilen des Zertifizierungsdienstes in einem anderen als in Satz 1 genannten Staat ist nur im Rahmen einer freiwilligen Akkreditierung zulässig, soweit die Sicherstellung der Aufsicht nachgewiesen wird.

§ 2

Inhalt des Sicherheitskonzepts

Das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 des Signaturgesetzes hat Folgendes zu enthalten:

1. eine Beschreibung aller erforderlichen technischen, baulichen und organisatorischen Sicherheitsmaßnahmen und deren Eignung,
2. eine Übersicht über die eingesetzten Produkte für qualifizierte elektronische Signaturen mit Herstellererklärungen nach § 17 Abs. 4 Satz 2 oder Bestätigungen nach § 17 Abs. 4 Satz 1 oder nach § 15 Abs. 7 Satz 1 des Signaturgesetzes,
3. eine Übersicht über die Aufbau- und Ablauforganisation sowie die Zertifizierungstätigkeit,
4. die Vorkehrungen und Maßnahmen zur Sicherstellung und Aufrechterhaltung des Betriebes, insbesondere bei Notfällen,
5. die Verfahren zur Beurteilung und Sicherstellung der Zuverlässigkeit des eingesetzten Personals und
6. eine Abschätzung und Bewertung verbleibender Sicherheitsrisiken.

§ 3

Identitätsprüfung und Attributsnachweise

(1) Der Zertifizierungsdiensteanbieter hat die Identifizierung des Antragstellers nach § 5 Abs. 1 des Signaturgesetzes anhand des Personalausweises oder eines Reisepasses, der auf eine Person mit Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes ausgestellt worden ist, oder anhand von Dokumenten mit gleichwertiger Sicherheit vorzunehmen. Soweit ein Antrag auf ein qualifiziertes Zertifikat mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments des Antragstellers gestellt wird, kann der Zertifizierungsdiensteanbieter von einer erneuten Identifizierung absehen. Die Identifizierung ist vor Übergabe des qualifizierten Zertifikats und vor Einstellung in das Zertifikatsverzeichnis gemäß § 4 Abs. 1 vorzunehmen.

(2) Sollen nach § 5 Abs. 2 des Signaturgesetzes in ein qualifiziertes Zertifikat Attribute aufgenommen werden, muss die nach § 5 Abs. 2 Satz 2 oder Satz 4 oder Abs. 3 Satz 2 des Signaturgesetzes erforderliche Einwilligung oder Bestätigung mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments oder schriftlich vorliegen. Die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle ist mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments oder schriftlich über den Inhalt des qualifizierten Zertifikates zu unterrichten und auf die Möglichkeit der Sperrung hinzuweisen.

§ 4

Führung eines Zertifikatsverzeichnisses

(1) Der Zertifizierungsdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens fünf weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen.

(2) Ein akkreditierter Zertifizierungdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen.

(3) Im Falle der Übernahme von qualifizierten Zertifikaten nach § 13 Abs. 1 Satz 2 des Signaturgesetzes gelten die Absätze 1 und 2 entsprechend.

§ 5

Einzelne Sicherheitsvorkehrungen des Zertifizierungsdiensteanbieters

(1) Der Zertifizierungsdiensteanbieter hat durch geeignete Maßnahmen sicherzustellen, dass Signaturschlüssel nur auf der jeweiligen sicheren Signaturerstellungseinheit oder bei ihm oder einem anderen Zertifizierungsdiensteanbieter unter Nutzung von technischen Komponenten nach § 17 Abs. 3 Nr. 1 des Signaturgesetzes erzeugt und auf sichere Signaturerstellungseinheiten übertragen werden. Soweit er auch Wissensdaten zur Identifikation des Signaturschlüssel-Inhabers gegenüber einer sicheren Signaturerstellungseinheit oder technische Komponenten zur Erfassung biometrischer Merkmale und Übertragung von Referenzdaten auf die sichere Signaturerstellungseinheit bereitstellt, hat er auch Vorkehrungen zu treffen, um die Geheimhaltung der Identifikationsdaten zu gewähr-

leisten und deren Speicherung außerhalb der jeweiligen sicheren Signaturerstellungseinheit nach Einbringen in dieselbe auszuschließen.

(2) Der Zertifizierungsdiensteanbieter hat von ihm bereitgestellte Signaturschlüssel und Identifikationsdaten dem Signaturschlüssel-Inhaber auf der sicheren Signaturerstellungseinheit persönlich zu übergeben und die Übergabe von diesem schriftlich oder als mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenes elektronisches Dokument bestätigen zu lassen, es sei denn, es wird schriftlich oder mittels einer qualifizierten elektronischen Signatur nach dem Signaturgesetz eine andere Übergabe vereinbart. Erst nachdem der Signaturschlüssel-Inhaber den Erhalt der sicheren Signaturerstellungseinheit gegenüber dem Zertifizierungsdiensteanbieter bestätigt hat, darf das zugehörige qualifizierte Zertifikat nach § 5 Abs. 1 Satz 2 und 3 des Signaturgesetzes nachprüfbar und, soweit vereinbart, abrufbar gehalten werden.

(3) Der Zertifizierungsdiensteanbieter hat sich zur Erfüllung der Voraussetzungen nach § 5 Abs. 5 des Signaturgesetzes von der Zuverlässigkeit von Personen, die am Zertifizierungsverfahren mitwirken, auf geeignete Weise zu überzeugen. Er kann hierzu insbesondere die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen. Unzuverlässige Personen sind vom Zertifizierungsverfahren auszuschließen. Der Zertifizierungsdiensteanbieter hat sich darüber hinaus anhand der Herstellerangaben oder in anderer geeigneter Weise von der Eignung der von ihm eingesetzten Produkte für qualifizierte elektronische Signaturen zu überzeugen und Vorkehrungen zu treffen, um diese vor unbefugtem Zugriff zu schützen.

§ 6

Ausgestaltung der Unterrichtung

Die Unterrichtung des Antragstellers nach § 6 Abs. 1 des Signaturgesetzes hat in allgemein verständlicher Sprache zu erfolgen und sich mindestens auf Folgendes zu erstrecken:

1. die Aufbewahrung und Anwendung der sicheren Signaturerstellungseinheit und geeignete Maßnahmen im Verlustfalle oder bei Verdacht des Mißbrauchs,
2. die Geheimhaltung von persönlichen Identifikationsnummern oder anderen Daten zur Identifikation des Signaturschlüssel-Inhabers gegenüber der sicheren Signaturerstellungseinheit,
3. die erforderlichen Sicherheitsmaßnahmen bei Erzeugung und Prüfung einer qualifizierten elektronischen Signatur,
4. die Möglichkeit von Beschränkungen in qualifizierten Zertifikaten nach § 7 Abs. 1 Nr. 7 des Signaturgesetzes,
5. die Notwendigkeit, Daten mit einer qualifizierten elektronischen Signatur neu zu signieren, falls die Signatur durch Zeitablauf ihren Sicherheitswert verliert,
6. die Existenz eines freiwilligen Akkreditierungssystems,
7. die dem Antragsteller zur Verfügung stehenden Beschwerde- und Schlichtungsmöglichkeiten sowie die Einzelheiten der Inanspruchnahme solcher Verfahren und
8. das Verfahren der Sperrung nach § 7.

Die Informationen sind auf Antrag auch Dritten zur Verfügung zu stellen.

§ 7

Sperrung von qualifizierten Zertifikaten

(1) Der Zertifizierungsdiensteanbieter hat den nach § 8 des Signaturgesetzes zur Sperrung Berechtigten eine Rufnummer bekannt zu geben, unter der diese unverzüglich eine Sperrung der qualifizierten Zertifikate veranlassen können.

(2) Der Zertifizierungsdiensteanbieter hat sich vor Sperrung auf geeignete Weise von der Identität des zur Sperrung Berechtigten zu überzeugen. Die Sperrung von qualifizierten Zertifikaten ist mit Angabe des Datums und der zu diesem Zeitpunkt gültigen gesetzlichen Zeit im Zertifikatsverzeichnis nach § 4 eindeutig kenntlich zu machen.

§ 8

Umfang der Dokumentation

(1) Die Dokumentation nach § 10 des Signaturgesetzes hat sich auf das Sicherheitskonzept, einschließlich aller Änderungen, die Unterlagen zur Fachkunde der im Betrieb tätigen Personen und die vertraglichen Vereinbarungen mit den Antragstellern zu erstrecken.

(2) Zum jeweiligen Antragsteller sind mindestens folgende Angaben und Unterlagen zu dokumentieren:

1. eine Ablichtung des vorgelegten Ausweises oder andere Identitätsnachweise,
2. ein vergebenes Pseudonym,
3. der Nachweis über die Unterrichtung des Antragstellers nach § 6 des Signaturgesetzes,
4. die Nachweise über die Einwilligungen der Berechtigten nach § 5 Abs. 2 Satz 2 und 4 und Abs. 3 Satz 2 des Signaturgesetzes,
5. die Bestätigungen der zuständigen Stellen nach § 5 Abs. 2 Satz 2 des Signaturgesetzes,
6. die ausgestellten qualifizierten Zertifikate mit dem jeweiligen Zeitpunkt der Ausstellung und der Übergabe sowie der Zeitpunkt der Einstellung in das Zertifikatsverzeichnis,
7. die Sperrung von qualifizierten Zertifikaten,
8. Auskünfte nach § 14 Abs. 2 Satz 2 des Signaturgesetzes und
9. die Übergabebestätigungen für Signaturschlüssel und Identifikationsdaten nach § 5 Abs. 2 Satz 1 oder die Erklärung des Signaturschlüssel-Inhabers, wenn er eine andere Übergabe verlangt hat, und gegebenenfalls einen anderen Nachweis.

(3) Die Dokumentation ist vorbehaltlich des Satzes 3 mindestens für den nach § 4 Abs. 1 genannten Zeitraum und bei akkreditierten Zertifizierungsdiensteanbietern mindestens für den nach § 4 Abs. 2 genannten Zeitraum aufzubewahren. Im Falle eines Gerichtsverfahrens, in dem der Nachweis der Zertifizierung von Belang ist, ist unbeschadet des Satzes 1 die Dokumentation mindestens bis zum rechtskräftigen Abschluss des Verfahrens aufzubewahren. Die Dokumentation von Auskünften nach § 14

Abs. 2 Satz 2 des Signaturgesetzes ist zwölf Monate aufzubewahren.

§ 9

Ausgestaltung der Deckungsvorsorge

(1) Die Deckungsvorsorge nach § 12 des Signaturgesetzes kann erbracht werden

1. durch eine Haftpflichtversicherung bei einem im Geltungsbereich dieses Gesetzes zum Geschäftsbetrieb befugten Versicherungsunternehmen oder
2. durch eine Freistellungs- oder Gewährleistungsverpflichtung eines im Geltungsbereich dieses Gesetzes zum Geschäftsbetrieb befugten Kreditinstituts, wenn gewährleistet ist, dass sie einer Haftpflichtversicherung vergleichbare Sicherheit bietet.

(2) Soweit die Deckungsvorsorge durch eine Versicherung nach Absatz 1 Nr. 1 erbracht wird, gelten die folgenden Bestimmungen:

1. Auf diese Versicherung finden § 158b Abs. 2 und die §§ 158c bis 158k des Gesetzes über den Versicherungsvertrag Anwendung. Zuständige Behörde nach § 158c Abs. 2 des Gesetzes über den Versicherungsvertrag ist die Behörde nach § 66 des Telekommunikationsgesetzes.
2. Die Mindestversicherungssumme muss 2,5 Millionen Euro für den einzelnen Versicherungsfall betragen. Versicherungsfall ist jedes auf den Einzelfall bezogene haftungsauslösende Ereignis im Sinne des § 12 Satz 1 des Signaturgesetzes, unabhängig von der Anzahl der dadurch ausgelösten Schadensfälle. Eine Vereinbarung, wonach ein Fehler, der sich in mehreren Zertifikaten, Zeitstempeln oder in der Auskunft nach § 5 Abs. 1 Satz 2 des Signaturgesetzes auswirkt, als ein Versicherungsfall gilt, ist nicht zulässig. Wird eine Jahreshöchstleistung für alle in einem Versicherungsjahr verursachten Schäden vereinbart, muss sie mindestens das Vierfache der Mindestversicherungssumme betragen.
3. Der räumliche Geltungsbereich des Versicherungsschutzes kann auf den Geltungsbereich der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000, Nr. L 13 S. 2) beschränkt werden.
4. Von der Versicherung kann die Leistung nur ausgeschlossen werden für Ersatzansprüche aus vorsätzlich begangener Pflichtverletzung des Zertifizierungsdiensteanbieters oder der Personen, für die er einzustehen hat.
5. Die Vereinbarung eines Selbstbehaltes bis zu 1 Prozent der Mindestversicherungssumme ist zulässig.

§ 10

Einstellen der Tätigkeit

(1) Der Zertifizierungsdiensteanbieter soll die Unterrichtung der zuständigen Behörde nach § 13 Abs. 1 Satz 1 des Signaturgesetzes spätestens zwei Monate vor Einstellung des Betriebes vornehmen.

(2) Der Zertifizierungsdiensteanbieter soll die Unterrichtung der Signaturschlüssel-Inhaber nach § 13 Abs. 1 Satz 3 des Signaturgesetzes mindestens zwei Monate vor Betriebsaufgabe vornehmen. Er hat den Signaturschlüssel-Inhabern mitzuteilen, ob ein anderer Zertifizierungsdiensteanbieter die Zertifikate übernimmt, und diesen zu benennen.

§ 11

Freiwillige Akkreditierung

(1) Der Antrag auf Akkreditierung nach § 15 Abs. 1 des Signaturgesetzes ist schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu stellen. Der Antrag auf freiwillige Akkreditierung gilt als Anzeige nach § 1, wenn die dort genannten Voraussetzungen erfüllt sind.

(2) Die Nachweise nach § 15 Abs. 1 Satz 2, Abs. 2 Satz 2 und Abs. 7 des Signaturgesetzes sind durch Vorlage der Ergebnisse der Prüf- und Bestätigungsstelle in schriftlicher Form oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu erbringen. Die regelmäßigen Prüfungen nach § 15 Abs. 2 Satz 2 des Signaturgesetzes sind im Abstand von drei Jahren durchzuführen. Der Prüfbericht und die Bestätigung darüber, dass die Anforderungen des Signaturgesetzes und dieser Verordnung weiterhin in vollem Umfang erfüllt werden, ist der zuständigen Behörde unaufgefordert vorzulegen.

(3) Bei der Prüfung und Bestätigung der Sicherheit von Produkten für qualifizierte elektronische Signaturen nach § 15 Abs. 7 Satz 1 des Signaturgesetzes sind die Vorgaben des Abschnitts I der Anlage 1 zu dieser Verordnung zu beachten.

§ 12

Festsetzung und Erhebung von Kosten

(1) Die gebührenpflichtigen Tatbestände für Amtshandlungen nach § 22 des Signaturgesetzes ergeben sich aus der Anlage 2 zu dieser Verordnung. Auslagen werden nach § 10 des Verwaltungskostengesetzes erhoben. Für den Widerruf oder die Rücknahme oder die Ablehnung eines Antrags oder einer Verwaltungshandlung werden Gebühren nach Maßgabe des § 15 des Verwaltungskostengesetzes erhoben.

(2) Für die Stundensätze nach Nummer 2 der Anlage 2 zu dieser Verordnung ist für jede angefangene Viertelstunde ein Viertel dieser Stundensätze zu berechnen. Werden öffentliche Leistungen durch Angehörige der zuständigen Behörde außerhalb der Behörde erbracht, so sind Gebühren ferner zu berechnen, die innerhalb der üblichen Arbeitszeit liegen oder von der zuständigen Behörde besonders abgegolten werden, sowie für Wartezeiten, die der Kostenschuldner verursacht hat.

§ 13

Festsetzung und Erhebung von Beiträgen

(1) Die Beiträge nach § 22 Abs. 2 Satz 1 des Signaturgesetzes berechnen sich nach dem hierfür erforderlichen Personal- und Sachaufwand der zuständigen Behörde unter Einschluss des Aufwandes für Investitionen. Der Beitragssatz beträgt 0,48 Euro für jedes vom Beitragspflichtigen ausgestellte qualifizierte Zertifikat. Der auf das

Allgemeininteresse entfallende Kostenanteil wurde beitragsmindernd berücksichtigt. Die Anteile am verbleibenden Aufwand werden den Beitragspflichtigen entsprechend der Zahl der von ihnen ausgestellten qualifizierten Zertifikate, die nach § 4 Abs. 1 im Zertifikatsverzeichnis zu führen sind, zugeordnet. Die Beitragspflichtigen haben der zuständigen Behörde die Zahl der Zertifikate nach Satz 2 jährlich, spätestens am 31. Januar des Folgejahres mitzuteilen. Kommt ein Beitragspflichtiger der Verpflichtung nach Satz 5 nicht nach, kann die zuständige Behörde eine Schätzung der ausgestellten qualifizierten Zertifikate eines Beitragspflichtigen vornehmen.

(2) Die Kosten des Investitionsaufwandes werden entsprechend den jeweils gültigen steuerlichen Regelungen zur Abschreibung von Investitionsgütern festgelegt.

(3) Für die Beiträge nach § 22 Abs. 2 Satz 2 des Signaturgesetzes gelten die Regelungen der Absätze 1 und 2, mit Ausnahme des Absatzes 1 Satz 4, entsprechend. Die Anteile am verbleibenden Aufwand nach Absatz 1 Satz 1 werden den Beitragspflichtigen entsprechend der Zahl der von ihnen ausgestellten qualifizierten Zertifikate, die nach § 4 Abs. 2 im Zertifikatsverzeichnis zu führen sind, zugeordnet.

(4) Die Beitragspflicht nach § 22 Abs. 2 Satz 1 des Signaturgesetzes beginnt mit dem Monat der Anzeige nach § 4 Abs. 3 des Signaturgesetzes, die Beitragspflicht nach § 22 Abs. 2 Satz 2 des Signaturgesetzes mit dem Monat der Akkreditierung. Die Beitragspflicht endet mit Ablauf des Monats der Einstellung der Tätigkeit nach § 13 Abs. 1 des Signaturgesetzes sowie bei freiwilliger Akkreditierung auch mit Ablauf des Monats des Widerrufs oder der Rücknahme einer Akkreditierung nach § 15 Abs. 5 des Signaturgesetzes. Der Beitrag wird jährlich erhoben. Maßgeblich ist das Kalenderjahr. Besteht die Beitragspflicht nicht das volle Kalenderjahr, so ist der Beitrag anteilig zu berechnen; die Sätze 1 und 2 gelten entsprechend. Die Beiträge werden nach den Vorschriften des Verwaltungsvollstreckungsgesetzes beigetrieben.

§ 14

Inhalt und Gültigkeitsdauer von qualifizierten Zertifikaten

(1) Die Angaben nach § 7 Abs. 1 des Signaturgesetzes in einem qualifizierten Zertifikat müssen eindeutig sein.

(2) Ein qualifiziertes Attribut-Zertifikat nach § 7 Abs. 2 des Signaturgesetzes muss außer einer eindeutigen Referenz auf das zugrunde liegende qualifizierte Zertifikat mindestens folgende Angaben enthalten und eine qualifizierte elektronische Signatur des Zertifizierungsdiensteanbieters tragen:

1. die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
2. die Nummer des Attribut-Zertifikates,
3. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
4. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
5. ein oder mehrere Attribute nach § 5 Abs. 2 des Signaturgesetzes.

(3) Die Gültigkeitsdauer eines qualifizierten Zertifikates darf höchstens fünf Jahre betragen und den Zeitraum der Eignung der eingesetzten Algorithmen und zugehörigen Parameter nicht überschreiten. Die Gültigkeit eines qualifizierten Attribut-Zertifikates endet spätestens mit der Gültigkeit des qualifizierten Zertifikates, auf das es Bezug nimmt.

§ 15

Anforderungen an Produkte für qualifizierte elektronische Signaturen

(1) Sichere Signaturerstellungseinheiten nach § 17 Abs. 1 Satz 1 des Signaturgesetzes müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann. Der Signaturschlüssel darf nicht preisgegeben werden. Bei Nutzung biometrischer Merkmale muss hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein. Die zur Erzeugung und Übertragung von Signaturschlüsseln erforderlichen technischen Komponenten nach § 17 Abs. 1 Satz 2 oder Abs. 3 Nr. 1 des Signaturgesetzes müssen gewährleisten, dass aus einem Signaturprüfschlüssel oder einer Signatur nicht der Signaturschlüssel errechnet werden kann und die Signaturschlüssel nicht dupliziert werden können.

(2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass

1. bei der Erzeugung einer qualifizierten elektronischen Signatur
   a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
   b) eine Signatur nur durch die berechtigt signierende Person erfolgt,
   c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und
2. bei der Prüfung einer qualifizierten elektronischen Signatur
   a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und
   b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

(3) Technische Komponenten nach § 17 Abs. 3 des Signaturgesetzes müssen gewährleisten, dass die Sperrung eines qualifizierten Zertifikates nicht unbemerkt rückgängig gemacht werden kann und die Auskünfte auf ihre Echtheit überprüft werden können. Die Auskünfte nach Satz 1 müssen beinhalten, ob die nachgeprüften qualifizierten Zertifikate im Verzeichnis der qualifizierten Zertifikate zum angegebenen Zeitpunkt vorhanden und ob sie nicht gesperrt waren. Nur nachprüfbar gehaltene qualifizierte Zertifikate dürfen nicht öffentlich abrufbar sein. Im Falle des § 17 Abs. 3 Nr. 3 des Signaturgesetzes muss gewährleistet sein, dass die zum Zeitpunkt der Erzeugung des qualifizierten Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird.

(4) Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

(5) Eine Herstellererklärung nach § 17 Abs. 4 des Signaturgesetzes muss

1. den Aussteller und das Produkt genau bezeichnen und
2. genaue Angaben darüber enthalten, welche Anforderungen des Signaturgesetzes und dieser Verordnung im Einzelnen erfüllt sind.

Bei der Prüfung und Bestätigung der Sicherheit von Produkten nach § 17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes sind die Vorgaben des Abschnitts II der Anlage 1 zu dieser Verordnung zu beachten.

(6) Soweit im Rahmen des Verfahrens nach Artikel 3 Abs. 5 und Artikel 9 der Richtlinie 1999/93/EG in der jeweils geltenden Fassung Referenznummern für allgemein anerkannte Normen für Produkte für qualifizierte elektronische Signaturen festgelegt und im Amtsblatt der Europäischen Gemeinschaften veröffentlicht werden, haben diese abweichend von den Absätzen 1 bis 5 Geltung, mit Ausnahme der Produkte nach § 15 Abs. 7 des Signaturgesetzes. Die zuständige Behörde veröffentlicht im Bundesanzeiger die aktuell gültigen Anforderungen auf Grund der Festlegungen nach Satz 1.

§ 16

Verfahren der Anerkennung sowie der Tätigkeit von Prüf- und Bestätigungsstellen

(1) Ein Antrag einer Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes muss Folgendes umfassen:

1. Namen und Anschrift des Antragstellers und seiner gesetzlichen Vertreter,
2. aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes des Antragstellers nach Nummer 1 und seiner gesetzlichen Vertreter,
3. einen aktuellen Handelsregisterauszug oder eine vergleichbare Unterlage,
4. Belege zum Nachweis der finanziellen Unabhängigkeit, insbesondere über Mindestkapital und vergleichbare Sicherheiten,
5. Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde nach § 18 Abs. 1 Satz 1 des Signaturgesetzes und
6. eine Erklärung, auf welche gesetzliche Tätigkeiten des Signaturgesetzes sich der Antrag bezieht.

(2) Für eine Anerkennung als Bestätigungsstelle für Tätigkeiten nach § 15 Abs. 7 und § 17 Abs. 4 Satz 1 des Signaturgesetzes muss der Antragsteller nachweisen, dass er über ausreichende Erfahrungen in der Anwendung der Prüfkriterien nach Anlage 1 zu dieser Verordnung verfügt. Er muss außerdem darlegen, wie er eine geeignete Überwachung der Prüftätigkeit sicherstellen wird.

(3) Die für die Tätigkeit als Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes und der Entscheidung der Kommission 2000/709/EG vom 6. November 2000 (ABl. EG Nr. L 289 S. 42) über die Mindestkriterien gemäß Artikel 3 Abs. 4 der Richtlinie 1999/93/EG erforderliche

1. Zuverlässigkeit besitzt, wer auf Grund seiner persönlichen Eigenschaften, seines Verhaltens und seiner Fähigkeiten zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist,
2. Unabhängigkeit besitzt, wer keinem wirtschaftlichen, finanziellen oder sonstigen Druck unterliegt, der sein Urteil beeinflussen oder das Vertrauen in die unparteiische Aufgabenwahrnehmung in Frage stellen kann,
3. Fachkunde besitzt, wer auf Grund seiner Ausbildung, beruflichen Bildung und praktischen Erfahrung zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist.

(4) Der Betreiber einer Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 des Signaturgesetzes hat sich von der Zuverlässigkeit und Fachkunde von Personen, die an der Prüfung oder Bestätigung mitwirken, auf geeignete Weise zu überzeugen. Er kann von diesen Personen die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen.

(5) Die zuständige Behörde veröffentlicht im Bundesanzeiger die Einzelheiten zu den Anforderungen nach den Absätzen 1 bis 4 und den Mindestkriterien nach Artikel 3 Abs. 4 der Richtlinie 1999/93/EG.

§ 17

Zeitraum und Verfahren zur langfristigen Datensicherung

Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

§ 18

Verfahren zur Feststellung der gleichwertigen Sicherheit von ausländischen elektronischen Signaturen und Produkten

(1) Ein Zertifizierungsdiensteanbieter, der nach § 23 Abs. 1 Satz 2 Nr. 2 des Signaturgesetzes für qualifizierte Zertifikate mit Rechtswirkung nach Artikel 5 Abs. 1 der Richtlinie 1999/93/EG eines außerhalb des Europäischen Wirtschaftsraumes (Drittstaat) niedergelassenen Zertifizierungsdiensteanbieters einsteht, hat dies der zuständigen Behörde spätestens zu dem Zeitpunkt, zu dem diese Zertifikate im Geltungsbereich des Signaturgesetzes rechtswirksam werden sollen, schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments anzuzeigen. Er hat dafür Sorge zu tragen, dass die qualifizierten Zertifikate des ausländischen Zertifizierungsdiensteanbieters und die darauf basierenden qualifizierten elektronischen Signaturen die Anforderungen des Signaturgesetzes und dieser Verordnung erfüllen und zu dem ausländischen Zertifizierungsdiensteanbieter die Unterlagen entsprechend § 1 Abs. 2 vorzulegen. § 2 gilt

für die Angaben zu dem ausländischen Zertifizierungsdiensteanbieter entsprechend. Die zuständige Behörde hat den Namen des ausländischen Zertifizierungsdiensteanbieters unter Angabe des Zertifizierungsdiensteanbieters, der für seine qualifizierten Zertifikate eintritt, nach § 19 Abs. 6 des Signaturgesetzes abrufbar zu halten.

(2) Die gleichwertige Sicherheit ausländischer elektronischer Signaturen nach § 23 Abs. 2 des Signaturgesetzes ist gegeben, wenn die zuständige Behörde festgestellt hat, dass

1. die Sicherheitsanforderungen an Zertifizierungsdiensteanbieter und Produkte für qualifizierte elektronische Signaturen,
2. die Prüfungsmodalitäten für Zertifizierungsdiensteanbieter und Produkte für qualifizierte elektronische Signaturen sowie die Anforderungen an die Prüf- und Bestätigungsstellen und
3. das Akkreditierungs- und Aufsichtssystem

eine gleichwertige Sicherheit bieten. Zur Feststellung der gleichwertigen Sicherheit kann die zuständige Behörde mit der zuständigen ausländischen Stelle die Verfahren zur Anerkennung vereinbaren, soweit nicht entsprechende überstaatliche oder zwischenstaatliche Vereinbarungen getroffen sind.

(3) Die Gleichwertigkeit von Produkten nach § 23 Abs. 3 Satz 2 des Signaturgesetzes ist gegeben, wenn die zuständige Behörde diese nach entsprechender Anwendung der Vorgaben nach Absatz 2 festgestellt hat.

(4) Die zuständige Behörde hat in ihr Verzeichnis nach § 16 Abs. 2 des Signaturgesetzes auch die qualifizierten Zertifikate für Signaturprüfschlüssel oberster ausländischer Zertifizierungsdiensteanbieter, die nach § 23 Abs. 2 des Signaturgesetzes als gleichwertig anerkannt sind, aufzunehmen. Sie hat die Anerkennung durch eine qualifizierte elektronische Signatur mit Anbieterakkreditierung nach § 15 des Signaturgesetzes zu bestätigen.

§ 19

Inkrafttreten, Außerkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft; gleichzeitig tritt die Signaturverordnung vom 22. Oktober 1997 (BGBl. I S. 2498), geändert durch die Verordnung vom 22. Juni 2000 (BGBl. I S. 981), außer Kraft.

Berlin, den 16. November 2001

Der Bundeskanzler
Gerhard Schröder

Der Bundesminister
für Wirtschaft und Technologie
Müller

Anlage 1
(zu § 11 Abs. 3, § 15 Abs. 5 und § 16 Abs. 2)

Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen

I. Zu § 11 Abs. 3 dieser Verordnung und nach § 15 Abs. 7 des Signaturgesetzes (freiwillige Akkreditierung)

1. Prüfvorgaben

1.1 Anforderungen an Prüftiefen

Die Prüfung der Produkte für qualifizierte elektronische Signaturen nach Maßgabe des § 15 Abs. 7 und des § 17 Abs. 4 des Signaturgesetzes hat nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (Common Criteria for Information Technology Security Evaluation, BAnz. 1999 S. 1945, – ISO/IEC 15408) oder nach den „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (ITSEC – GMBl vom 8. August 1992, S. 545) in der jeweils geltenden Fassung zu erfolgen.

Die Prüfung muss

a) bei technischen Komponenten nach § 2 Nr. 12 Buchstabe a des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen,

b) bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen,

c) i) bei technischen Komponenten für Zertifizierungsdienste nach § 2 Nr. 12 Buchstabe b und c des Signaturgesetzes, die außerhalb eines besonders gesicherten Bereichs („Trustcenter“) eingesetzt werden, mindestens die Prüfstufe „EAL 4“ oder „E3“ umfassen,

ii) bei technischen Komponenten für Zertifizierungsdienste nach § 2 Nr. 12 Buchstabe b und c des Signaturgesetzes, die innerhalb eines besonders gesicherten Bereichs eingesetzt werden, mindestens die Prüfstufe „EAL 3“ oder „E 2“ umfassen,

d) bei Signaturanwendungskomponenten nach § 2 Nr. 11 des Signaturgesetzes mindestens die Prüfstufe „EAL 3“ oder „E 2“ umfassen.

1.2 Anforderungen an Schwachstellenbewertung/Mechanismenstärke

Bei den Prüfstufen „EAL 4“ und bei „EAL 3“ gemäß Abschnitt I Nr. 1.1 Buchstabe a bis c i) und Buchstabe d ist ergänzend zu den bei dieser Prüfstufe vorgeschriebenen Maßnahmen gegen ein hohes Angriffspotenzial zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen.

Die Stärke der Sicherheitsmechanismen muss bei allen Produkten gemäß Abschnitt I Nr. 1.1 Buchstabe a bis d im Fall „E 3“ und „E 2“ mit „hoch“ bewertet werden.

Abweichend hiervon genügt für den Mechanismus zur Identifikation durch biometrische Merkmale eine Bewertung der Sicherheitsmechanismen mit „mittel“, wenn diese zusätzlich zur Identifikation durch Wissensdaten genutzt werden.

1.3 Anforderungen an Algorithmen

Die Algorithmen und zugehörigen Parameter müssen nach Abschnitt I Nr. 1.2 dieser Anlage als geeignet beurteilt sein.

2. Algorithmen – Veröffentlichung und Neubestimmung der Eignung

Die zuständige Behörde veröffentlicht im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt. Der Zeitpunkt soll mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und Veröffentlichung liegen. Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen. Die Eignung ist gegeben, wenn innerhalb des bestimmten Zeitraumes nach dem Stand von Wissenschaft und Technik eine nicht feststellbare Fälschung von qualifizierten elektronischen Signaturen oder Verfälschung von signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann. Die Eignung wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Berücksichtigung internationaler Standards festgestellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

3. Sicherheitsbestätigungen für Signaturprodukte

In der Bestätigung der Erfüllung der Anforderungen für Produkte für qualifizierte elektronische Signaturen ist anzugeben,

a) für welche Anforderungen nach § 17 des Signaturgesetzes und nach § 15 dieser Verordnung die Bestätigung gilt und unter welchen Einsatzbedingungen,

b) welche Algorithmen und zugehörigen Parameter nach Abschnitt I Nr. 2 eingesetzt und bis zu welchem Zeitpunkt diese mindestens geeignet sind sowie

c) nach welcher Stufe die Produkte geprüft wurden und welche Mechanismenstärke erreicht wurde.

Eine Ausfertigung des Prüfberichtes, der Bewertung durch die Bestätigungsstelle und der Bestätigung ist bei der zuständigen Behörde zu hinterlegen. Auf Anforderung sind dieser auch alle weiteren Prüfunterlagen vorzulegen. Sie kann bei Anhaltspunkten für Mängel bei Prüfungen oder bei bestätigten Produkten sowie stichprobenweise Gutachten eines unabhängigen Dritten darüber einholen, ob die Produkte gemäß dieser Anlage geprüft wurden und ob diese die Anforderungen des Signaturgesetzes und der Signaturverordnung erfüllen. Betroffene Hersteller, Vertreiber und Prüfstellen haben die dafür erforderliche Unterstützung zu gewähren. Wird diese nicht gewährt oder stellt sich heraus, dass bestätigte Produkte nicht ausreichend geprüft wurden oder Anforderungen nicht erfüllen, so kann die zuständige Behörde erteilte Bestätigungen für ungültig erklären.

4. Veröffentlichung der Sicherheitsbestätigung für Produkte

Die zuständige Behörde hat Produkte für qualifizierte elektronische Signaturen, die von einer nach § 18 des Signaturgesetzes anerkannten Stelle eine Bestätigung gemäß Abschnitt I Nr. 3 erhalten haben, im Bundesanzeiger zu veröffentlichen. Dabei ist anzugeben, bis zu welchem Zeitpunkt die Bestätigung mindestens gilt. Wird eine Bestätigung für ungültig erklärt, so hat die zuständige Behörde dies unter Angabe des Zeitpunktes, ab dem diese Maßnahme gilt, ebenfalls im Bundesanzeiger zu veröffentlichen.

II. Zu § 15 Abs. 5 dieser Verordnung und nach § 17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes (nach § 4 Abs. 3 des Signaturgesetzes angezeigte Zertifizierungsdiensteanbieter ohne freiwillige Akkreditierung)

Für die Prüfung von Produkten nach § 15 Abs. 5 gelten die Anforderungen nach Abschnitt I entsprechend.

Abweichend hiervon können

– Produkte zum Einsatz kommen, die den Normen nach § 15 Abs. 6 entsprechen,

– Produkte nach § 17 Abs. 2 und 3 Nr. 2 und 3 des Signaturgesetzes (bzw. nach Abschnitt I Nr. 1.1 Buchstabe c und d) zum Einsatz kommen, bei denen anstelle der Bestätigung eine Herstellererklärung nach § 17 Abs. 4 des Signaturgesetzes vorliegt.

Anlage 2
(zu § 12)

Kosten

Kosten für Amtshandlungen nach § 22 Abs. 1 des Signaturgesetzes

1.1 Kosten nach § 22 Abs. 1 Nr. 1 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
1	Prüfung und Erteilung einer Akkreditierung nach § 15 Abs. 1 des Signaturgesetzes	Gebühr nach Zeitaufwand
2	Ablehnung eines Antrages auf Akkreditierung nach § 15 Abs. 4 des Signaturgesetzes oder Rücknahme oder Widerruf einer Akkreditierung nach § 15 Abs. 5 des Signaturgesetzes	Gebühr nach Zeitaufwand
3	Vollständige oder teilweise Zurückweisung eines Widerspruchs im Rahmen des Verfahrens nach § 15 Abs. 1 bis 6 des Signaturgesetzes	2 500
4	Überprüfung von Prüfberichten und Bestätigungen nach § 15 Abs. 2 des Signaturgesetzes	3 500
5	Maßnahmen im Falle des Widerrufs oder der Rücknahme einer Akkreditierung oder im Falle der Einstellung der Tätigkeit eines akkreditierten Zertifizierungsdiensteanbieters nach § 15 Abs. 6 des Signaturgesetzes	Gebühr nach Zeitaufwand
6	Prüfungen und andere Maßnahmen nach § 19 des Signaturgesetzes	Gebühr nach Zeitaufwand

1.2 Kosten nach § 22 Abs. 1 Nr. 2 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
7	Ausstellung eines qualifizierten Zertifikates sowie dessen Sperrung nach § 16 Abs. 1des Signaturgesetzes	500
8	Ausstellung einer Bescheinigung nach § 16 Abs. 3 des Signaturgesetzes	500

1.3 Kosten nach § 22 Abs. 1 Nr. 3 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
	Erteilung einer Anerkennung als Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes nach	
9	a) § 15 Abs. 2 des Signaturgesetzes	2 500
10	b) § 15 Abs. 7 des Signaturgesetzes	2 500
11	c) § 17 Abs. 3 des Signaturgesetzes	1 000
	Ablehnung eines Antrages auf Anerkennung oder Rücknahme oder Widerruf einer Anerkennung für Tätigkeiten nach	
12	a) § 15 Abs. 2 des Signaturgesetzes	2 500
13	b) § 15 Abs. 7 des Signaturgesetzes	2 500
14	c) § 17 Abs. 4 des Signaturgesetzes	1 000
15	Vollständige oder teilweise Zurückweisung eines Widerspruchs im Rahmen des Verfahrens nach § 18 Abs. 1 des Signaturgesetzes	1 000

1.4 Kosten nach § 22 Abs. 1 Nr. 4 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
16	Bearbeitung einer Anzeige nach § 4 Abs. 2 und 3 des Signaturgesetzes und erstmalige Überprüfung der Einhaltung des Signaturgesetzes und dieser Verordnung nach § 19 des Signaturgesetzes	Gebühr nach Zeitaufwand
17	Stichprobenartige Prüfungen im Rahmen der Aufsicht nach § 19 Abs. 1 des Signaturgesetzes im Falle der Feststellung eines Verstoßes gegen die für den Betrieb eines Zertifizierungsdienstes maßgeblichen Vorschriften des Signaturgesetzes oder dieser Verordnung	Gebühr nach Zeitaufwand
18	Anlassbezogene Prüfungen und andere Maßnahmen nach § 19 Abs. 1 des Signaturgesetzes im Falle eines Verstoßes gegen die für den Betrieb eines Zertifizierungsdienstes maßgeblichen Vorschriften des Signaturgesetzes oder dieser Verordnung	Gebühr nach Zeitaufwand

1.5 Kosten nach § 23 Abs. 1 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
19	Bearbeitung einer Anzeige nach § 18 Abs. 1 Satz 1 dieser Verordnung einschließlich der Aufnahme in das Zertifikatsverzeichnis nach § 18 Abs. 1 Satz 4 dieser Verordnung	Gebühr nach Zeitaufwand

2. Stundensätze und Km-Pauschale für Kfz-Einsatz

Kosten-nummer	Stundensatz/Km-Pauschale	Euro
20	Beamte des höheren Dienstes oder vergleichbare Angestellte	125
21	Beamte des gehobenen Dienstes oder vergleichbare Angestellte	95
22	Beamte des mittleren Dienstes oder vergleichbare Angestellte	69
23	Kraftfahrzeugeinsatz	0,70 Euro/km

Formvorschriften

Im folgenden das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001.

Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr

Vom 13. Juli 2001

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Bürgerlichen Gesetzbuchs

Das Bürgerliche Gesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 400-2, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 2 Abs. 25 des Gesetzes vom 25. Juni 2001 (BGBl. I S. 1206), wird wie folgt geändert:

1. In § 120 wird das Wort „Anstalt“ durch das Wort „Einrichtung“ ersetzt.

2. § 126 wird wie folgt geändert:

   a) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

   „(3) Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.“

   b) Der bisherige Absatz 3 wird Absatz 4.

3. Nach § 126 werden folgende §§ 126a und 126b eingefügt:

„§ 126a

(1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

§ 126b

Ist durch Gesetz Textform vorgeschrieben, so muss die Erklärung in einer Urkunde oder auf andere zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben, die Person des Erklärenden genannt und der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht werden.“

4. § 127 wird wie folgt gefasst:

„§ 127

(1) Die Vorschriften des § 126, des § 126a oder des § 126b gelten im Zweifel auch für die durch Rechtsgeschäft bestimmte Form.

(2) Zur Wahrung der durch Rechtsgeschäft bestimmten schriftlichen Form genügt, soweit nicht ein anderer Wille anzunehmen ist, die telekommunikative Übermittlung und bei einem Vertrag der Briefwechsel. Wird eine solche Form gewählt, so kann nachträglich eine dem § 126 entsprechende Beurkundung verlangt werden.

(3) Zur Wahrung der durch Rechtsgeschäft bestimmten elektronischen Form genügt, soweit nicht ein anderer Wille anzunehmen ist, auch eine andere als die in § 126a bestimmte elektronische Signatur und bei einem Vertrag der Austausch von Angebots- und Annahmeerklärung, die jeweils mit einer elektronischen Signatur versehen sind. Wird eine solche Form gewählt, so kann nachträglich eine dem § 126a entsprechende elektronische Signierung oder, wenn diese einer der Parteien nicht möglich ist, eine dem § 126 entsprechende Beurkundung verlangt werden.“

5. In § 147 Abs. 1 Satz 2 werden nach den Wörtern „mittels Fernsprechers“ die Wörter „oder einer sonstigen technischen Einrichtung“ eingefügt.

6. In § 541b Abs. 2 Satz 1, §§ 552a und 651g Abs. 2 Satz 3 wird jeweils das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

7. In § 623 werden der Punkt durch ein Semikolon ersetzt und die Wörter „die elektronische Form ist ausgeschlossen.“ angefügt.

8. Dem § 630 wird folgender Satz angefügt:

   „Die Erteilung des Zeugnisses in elektronischer Form ist ausgeschlossen.“

8a. Dem § 761 wird folgender Satz angefügt:

   „Die Erteilung des Leibrentenversprechens in elektronischer Form ist ausgeschlossen, soweit das Versprechen der Gewährung familienrechtlichen Unterhaltes dient.“

9. Nach § 766 Satz 1 wird folgender Satz eingefügt:

„Die Erteilung der Bürgschaftserklärung in elektronischer Form ist ausgeschlossen."

10. Dem § 780 wird folgender Satz angefügt:

„Die Erteilung des Versprechens in elektronischer Form ist ausgeschlossen."

11. Nach § 781 Satz 1 wird folgender Satz eingefügt:

„Die Erteilung der Anerkennungserklärung in elektronischer Form ist ausgeschlossen."

Artikel 2

Änderung der Zivilprozessordnung

Die Zivilprozessordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 310-4, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 25. Juni 2001 (BGBl. I S. 1206), wird wie folgt geändert:

1. § 130 Nr. 6 wird wie folgt gefasst:

„6. die Unterschrift der Person, die den Schriftsatz verantwortet, bei Übermittlung durch einen Telefaxdienst (Telekopie) die Wiedergabe der Unterschrift in der Kopie."

2. Nach § 130 wird folgender § 130a eingefügt:

„§ 130a

Elektronisches Dokument

(1) Soweit für vorbereitende Schriftsätze und deren Anlagen, für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist. Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.

(3) Ein elektronisches Dokument ist eingereicht, sobald die für den Empfang bestimmte Einrichtung des Gerichts es aufgezeichnet hat."

3. In § 133 Abs. 2 werden die Wörter „auf der Geschäftsstelle niederzulegen" durch die Wörter „bei dem Gericht einzureichen" ersetzt.

4. Nach § 292 wird folgender § 292a eingefügt:

„§ 292a

Anscheinsbeweis bei qualifizierter elektronischer Signatur

Der Anschein der Echtheit einer in elektronischer Form (§ 126a des Bürgerlichen Gesetzbuchs) vorliegenden Willenserklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist."

4a. § 299 wird wie folgt geändert:

a) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Soweit die Prozessakten als elektronische Dokumente vorliegen, ist die Akteneinsicht auf Ausdrucke beschränkt. Die Ausdrucke sind von der Geschäftsstelle zu fertigen."

b) Der bisherige Absatz 3 wird Absatz 4.

5. § 299a wird wie folgt gefasst:

„§ 299a

Sind die Prozessakten nach ordnungsgemäßen Grundsätzen zur Ersetzung der Urschrift auf einen Bild- oder anderen Datenträger übertragen worden und liegt der schriftliche Nachweis darüber vor, dass die Wiedergabe mit der Urschrift übereinstimmt, so können Ausfertigungen, Auszüge und Abschriften von dem Bild- oder dem Datenträger erteilt werden. Auf der Urschrift anzubringende Vermerke werden in diesem Fall bei dem Nachweis angebracht."

6. Dem § 371 wird folgender Satz 2 angefügt:

„Ist ein elektronisches Dokument Gegenstand des Beweises, wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten; befindet diese sich nicht im Besitz des Beweisführers, gelten die §§ 422 bis 432 entsprechend."

Artikel 3

Änderung des Bundeskleingartengesetzes

Das Bundeskleingartengesetz vom 28. Februar 1983 (BGBl. I S. 210), zuletzt geändert durch Artikel 7 Abs. 15 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1149), wird wie folgt geändert:

1. In § 5 Abs. 3 Satz 1 wird das Wort „schriftlich" durch die Wörter „in Textform" ersetzt.

2. In § 8 Nr. 1 werden die Wörter „schriftlicher Mahnung" durch die Wörter „Mahnung in Textform" ersetzt.

3. In § 9 Abs. 1 Nr. 1 werden die Wörter „schriftlichen Abmahnung" durch die Wörter „in Textform abgegebenen Abmahnung" ersetzt.

4. In § 12 Abs. 2 Satz 2 wird das Wort „schriftlich" durch die Wörter „in Textform" ersetzt.

Artikel 4
Änderung des Gesetzes zur Änderung des Bundeskleingartengesetzes

In Artikel 3 Satz 4 des Gesetzes zur Änderung des Bundeskleingartengesetzes vom 8. April 1994 (BGBl. I S. 766), das durch Artikel 7 Abs. 16 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1149) geändert worden ist, werden die Wörter „schriftliche Erklärung“ durch die Wörter „in Textform abgegebene Erklärung“ ersetzt.

Artikel 5
Änderung des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit

§ 21 des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit in der im Bundesgesetzblatt Teil III, Gliederungsnummer 315-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 2 Abs. 5 des Gesetzes vom 19. Februar 2001 (BGBl. I S. 288, 436) geändert worden ist, wird wie folgt geändert:

1. Dem Absatz 2 wird folgender Satz angefügt:

   „Die Beschwerde kann auch entsprechend den Regelungen der Zivilprozessordnung betreffend die Übermittlung von Anträgen und Erklärungen als elektronisches Dokument eingelegt werden.“

2. Nach Absatz 2 wird folgender Absatz 3 angefügt:

   „(3) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.“

Artikel 5a
Änderung der Grundbuchordnung

Die Grundbuchordnung in der Fassung der Bekanntmachung vom 26. Mai 1994 (BGBl. I S. 1114), zuletzt geändert durch Artikel 2 Abs. 13 des Gesetzes vom 25. Juni 2001 (BGBl. I S. 1206), wird wie folgt geändert:

1. Dem § 73 Abs. 2 wird folgender Satz angefügt:

   „Die Beschwerde kann auch entsprechend den Regelungen der Zivilprozessordnung betreffend die Übermittlung von Anträgen und Erklärungen als elektronisches Dokument eingelegt werden.“

2. Nach § 81 Abs. 2 wird folgender Absatz 3 angefügt:

   „(3) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.“

Artikel 5b
Änderung der Schiffsregisterordnung

Die Schiffsregisterordnung in der Fassung der Bekanntmachung vom 26. Mai 1994 (BGBl. I S. 1133), geändert durch Artikel 5 Abs. 1 des Gesetzes vom 6. Juni 1995 (BGBl. I S. 778), wird wie folgt geändert:

1. Dem § 77 Abs. 2 wird folgender Satz angefügt:

   „Die Beschwerde kann auch entsprechend den Regelungen der Zivilprozessordnung betreffend die Übermittlung von Anträgen und Erklärungen als elektronisches Dokument eingelegt werden.“

2. Nach § 89 Abs. 2 wird folgender Absatz 3 angefügt:

   „(3) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.“

Artikel 6
Änderung des Grundbuchbereinigungsgesetzes

In § 5 Abs. 1 Satz 1 des Grundbuchbereinigungsgesetzes vom 20. Dezember 1993 (BGBl. I S. 2182, 2192), das zuletzt durch Artikel 5 des Gesetzes vom 2. November 2000 (BGBl. I S. 1481) geändert worden ist, wird das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

Artikel 6a
Änderung des Gesetzes über das gerichtliche Verfahren in Landwirtschaftssachen

Das Gesetz über das gerichtliche Verfahren in Landwirtschaftssachen in der im Bundesgesetzblatt Teil III, Gliederungsnummer 317-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 2 Abs. 14 des Gesetzes vom 25. Juni 2001 (BGBl. I S. 1206), wird wie folgt geändert:

1. Dem § 26 Abs. 1 wird folgender Satz angefügt:

   „Die Beschwerde kann auch entsprechend den Regelungen der Zivilprozessordnung betreffend die Übermittlung von Anträgen und Erklärungen als elektronisches Dokument eingelegt werden.“

2. Nach § 26 Abs. 5 wird folgender Absatz 6 angefügt:

   „(6) Die Bundesregierung bestimmt durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente beim Bundesgerichtshof eingereicht

werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Zulassung der elektronischen Form kann auf einzelne Verfahren beschränkt werden."

Artikel 6b

Änderung des Arbeitsgerichtsgesetzes

Das Arbeitsgerichtsgesetz in der Fassung der Bekanntmachung vom 2. Juli 1979 (BGBl. I S. 853, 1036), zuletzt geändert durch Artikel 2 Abs. 16 des Gesetzes vom 25. Juni 2001 (BGBl. I S. 1206), wird wie folgt geändert:

Nach § 46a wird folgender § 46b eingefügt:

„§ 46b

Einreichung elektronischer Dokumente

(1) Soweit für vorbereitende Schriftsätze und deren Anlagen, für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist. Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die jeweils zuständige oberste Landesbehörde übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.

(3) Ein elektronisches Dokument ist eingereicht, sobald die für den Empfang bestimmte Einrichtung des Gerichts es aufgezeichnet hat."

Artikel 7

Änderung des Sozialgerichtsgesetzes

Das Sozialgerichtsgesetz in der Fassung der Bekanntmachung vom 23. September 1975 (BGBl. I S. 2535), zuletzt geändert durch Artikel 2 Abs. 17 des Gesetzes vom 25. Juni 2001 (BGBl. I S. 1206), wird wie folgt geändert:

1. Nach § 108 wird folgender § 108a eingefügt:

„§ 108a

(1) Soweit für vorbereitende Schriftsätze und deren Anlagen, für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist. Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die für die Sozialgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.

(3) Ein elektronisches Dokument ist eingereicht, sobald die für den Empfang bestimmte Einrichtung des Gerichts es aufgezeichnet hat."

2. In § 120 Abs. 2 Satz 2 werden die Wörter „einem Bildträger verkleinert wiedergegeben" durch die Wörter „einen Bild- oder anderen Datenträger übertragen" ersetzt.

Artikel 8

Änderung der Verwaltungsgerichtsordnung

Die Verwaltungsgerichtsordnung in der Fassung der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), zuletzt geändert durch Artikel 14 des Gesetzes vom 9. Juli 2001 (BGBl. I S. 1510), wird wie folgt geändert:

1. Nach § 86 wird folgender § 86a eingefügt:

„§ 86a

(1) Soweit für vorbereitende Schriftsätze und deren Anlagen, für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist. Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die für die Verwaltungsgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.

(3) Ein elektronisches Dokument ist eingereicht, sobald die für den Empfang bestimmte Einrichtung des Gerichts es aufgezeichnet hat."

2. In § 100 Abs. 2 Satz 2 werden die Wörter „einem Bildträger verkleinert wiedergegeben" durch die Wörter „einen Bild- oder anderen Datenträger übertragen" ersetzt.

Artikel 9

Änderung der Finanzgerichtsordnung

Die Finanzgerichtsordnung in der Fassung der Bekanntmachung vom 28. März 2001 (BGBl. I S. 442), geändert durch Artikel 2 Abs. 19 des Gesetzes vom 25. Juni 2001 (BGBl. I S. 1206), wird wie folgt geändert:

1. Nach § 77 wird folgender § 77a eingefügt:

„§ 77a

(1) Soweit für vorbereitende Schriftsätze und deren Anlagen, für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist. Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die für die Finanzgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.

(3) Ein elektronisches Dokument ist eingereicht, sobald die für den Empfang bestimmte Einrichtung des Gerichts es aufgezeichnet hat.“

2. In § 78 Abs. 1 Satz 2 werden die Wörter „einem Bildträger verkleinert wiedergegeben“ durch die Wörter „einen Bild- oder anderen Datenträger übertragen“ ersetzt.

Artikel 10

Änderung des Gerichtskostengesetzes

Das Gerichtskostengesetz in der Fassung der Bekanntmachung vom 15. Dezember 1975 (BGBl. I S. 3047), zuletzt geändert durch Artikel 13 des Gesetzes vom 9. Juli 2001 (BGBl. I S. 1510), wird wie folgt geändert:

1. In § 5 Abs. 3 Satz 1 wird die Angabe „§ 129a der Zivilprozessordnung gilt“ durch die Angabe „§§ 129a, 130a der Zivilprozessordnung gelten“ ersetzt.

2. In § 23 Abs. 1 werden der Punkt durch ein Semikolon ersetzt und die Wörter „§ 130a der Zivilprozessordnung gilt entsprechend.“ angefügt.

Artikel 11

Änderung der Kostenordnung

In § 14 Abs. 4 der Kostenordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 361-1, veröffentlichten bereinigten Fassung, die zuletzt durch Artikel 2 Abs. 21 des Gesetzes vom 25. Juni 2001 (BGBl. I S. 1206) geändert worden ist, werden der Punkt durch ein Semikolon ersetzt und die Wörter „§ 130a der Zivilprozessordnung gilt entsprechend.“ angefügt.

Artikel 12

Änderung des Gesetzes über die Entschädigung der ehrenamtlichen Richter

In § 12 Abs. 4 des Gesetzes über die Entschädigung der ehrenamtlichen Richter in der Fassung der Bekanntmachung vom 1. Oktober 1969 (BGBl. I S. 1753), das zuletzt durch Artikel 4 des Gesetzes vom 27. April 2001 (BGBl. I S. 751) geändert worden ist, werden der Punkt durch ein Semikolon ersetzt und die Wörter „§ 130a der Zivilprozessordnung gilt entsprechend.“ angefügt.

Artikel 13

Änderung des Gesetzes über die Entschädigung von Zeugen und Sachverständigen

In § 16 Abs. 3 des Gesetzes über die Entschädigung von Zeugen und Sachverständigen in der Fassung der Bekanntmachung vom 1. Oktober 1969 (BGBl. I S. 1756), das zuletzt durch Artikel 5 des Gesetzes vom 27. April 2001 (BGBl. I S. 751) geändert worden ist, werden der Punkt durch ein Semikolon ersetzt und die Wörter „§ 130a der Zivilprozessordnung gilt entsprechend.“ angefügt.

Artikel 14

Änderung der Bundesgebührenordnung für Rechtsanwälte

In § 10 Abs. 4 der Bundesgebührenordnung für Rechtsanwälte in der im Bundesgesetzblatt Teil III, Gliederungsnummer 368-1, veröffentlichten bereinigten Fassung, die zuletzt durch Artikel 15 des Gesetzes vom 9. Juli 2001 (BGBl. I S. 1510) geändert worden ist, werden der Punkt durch ein Semikolon ersetzt und die Wörter „§ 130a der Zivilprozessordnung gilt entsprechend.“ angefügt.

Artikel 15

Änderung der Nutzungsentgeltverordnung

In § 6 Abs. 1 der Nutzungsentgeltverordnung vom 22. Juli 1993 (BGBl. I S. 1339), die durch die Verordnung vom 24. Juli 1997 (BGBl. I S. 1920) geändert worden ist, wird jeweils das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

Artikel 16

Änderung des Verbraucherkreditgesetzes

Das Verbraucherkreditgesetz in der Fassung der Bekanntmachung vom 29. Juni 2000 (BGBl. I S. 940) wird wie folgt geändert:

1. Nach § 4 Abs. 1 Satz 2 wird folgender Satz eingefügt:

„Der Abschluss des Vertrages in elektronischer Form ist ausgeschlossen.“

2. In § 5 Abs. 1 werden die Sätze 3 bis 5 durch die folgenden Sätze 3 und 4 ersetzt:

   „Die Vertragsbedingungen der Nummern 1 bis 4 sind dem Verbraucher spätestens nach der ersten Inanspruchnahme des Kredits zu bestätigen; ferner ist der Verbraucher während der Inanspruchnahme des Kredits über jede Änderung des Jahreszinses zu unterrichten. Die Bestätigung und die Unterrichtung nach Satz 3 haben in Textform zu erfolgen."

Artikel 17

Änderung des Gesetzes zur Regelung der Miethöhe

Das Gesetz zur Regelung der Miethöhe vom 18. Dezember 1974 (BGBl. I S. 3603, 3604), zuletzt geändert durch Artikel 10 des Gesetzes vom 9. Juni 1998 (BGBl. I S. 1242), wird wie folgt geändert:

1. In § 2 Abs. 2 Satz 1 wird das Wort „schriftlich" durch die Wörter „in Textform" ersetzt.

2. In § 3 Abs. 3 Satz 1, § 4 Abs. 2 Satz 1 und Abs. 5 Satz 1, § 5 Abs. 1, § 6 Abs. 2 Satz 1, § 7 Abs. 2 Satz 1 und § 10a Abs. 3 Satz 1 werden jeweils die Wörter „schriftliche Erklärung" durch die Wörter „Erklärung in Textform" ersetzt.

3. § 8 wird aufgehoben.

Artikel 18

Änderung des Schuldrechtsanpassungsgesetzes

Das Schuldrechtsanpassungsgesetz vom 21. September 1994 (BGBl. I S. 2538), zuletzt geändert durch Artikel 7 Abs. 24 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1149), wird wie folgt geändert:

1. In § 20 Abs. 3 Satz 3 und § 47 Abs. 3 Satz 2 wird jeweils das Wort „schriftlich" durch die Wörter „in Textform" ersetzt.

2. In § 35 Abs. 1 Satz 2 werden die Wörter „schriftliche Anforderung" durch die Wörter „in Textform vorzulegende Anforderung" ersetzt.

Artikel 19

Änderung des Teilzeit-Wohnrechtegesetzes

Nach § 3 Abs. 1 Satz 1 des Teilzeit-Wohnrechtegesetzes in der Fassung der Bekanntmachung vom 29. Juni 2000 (BGBl. I S. 957) wird folgender Satz eingefügt:

„Der Abschluss des Vertrages in elektronischer Form ist ausgeschlossen."

Artikel 20

Änderung des Wohnungseigentumsgesetzes

In § 24 Abs. 4 Satz 1 des Wohnungseigentumsgesetzes in der im Bundesgesetzblatt Teil III, Gliederungsnummer 403-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 7 Abs. 25 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1149) geändert worden ist, wird das Wort „schriftlich" durch die Wörter „in Textform" ersetzt.

Artikel 21

Änderung des Sachenrechtsbereinigungsgesetzes

In § 31 Abs. 4 Satz 2 des Sachenrechtsbereinigungsgesetzes vom 21. September 1994 (BGBl. I S. 2457), das zuletzt durch Artikel 7 Abs. 27 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1149) geändert worden ist, wird das Wort „schriftlich" durch die Wörter „in Textform" ersetzt.

Artikel 22

Änderung des Handelsgesetzbuchs

Das Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 16 des Gesetzes vom 26. Juni 2001 (BGBl. I S. 1310), wird wie folgt geändert:

1. Dem § 73 wird folgender Satz angefügt:

   „Die Erteilung des Zeugnisses in elektronischer Form ist ausgeschlossen."

2. § 100 Abs. 1 Satz 3 wird wie folgt gefasst:

   „Das Eingetragene ist von dem Handelsmakler täglich zu unterzeichnen oder gemäß § 126a Abs. 1 des Bürgerlichen Gesetzbuchs elektronisch zu signieren."

3. In § 350 werden die Angabe „§ 766 Satz 1" durch die Angabe „§ 766 Satz 1 und 2" und die Angabe „§ 781 Satz 1" durch die Angabe „§ 781 Satz 1 und 2" ersetzt.

4. In § 410 Abs. 1, § 455 Abs. 1 Satz 2 und § 468 Abs. 1 Satz 1 werden jeweils die Wörter „schriftlich oder in sonst lesbarer Form" durch die Wörter „in Textform" ersetzt.

5. § 438 Abs. 4 wird wie folgt gefasst:

   „(4) Eine Schadensanzeige nach Ablieferung ist in Textform zu erstatten. Zur Wahrung der Frist genügt die rechtzeitige Absendung."

Artikel 23

Änderung des Börsengesetzes

Das Börsengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2682), geändert durch Artikel 3 Abs. 2 des Gesetzes vom 21. Dezember 2000 (BGBl. I S. 1857), wird wie folgt geändert:

1. In § 45 Abs. 4 werden die Wörter „schriftliche Darstellung", in § 73 Abs. 2 die Wörter „schriftlichen Darstellung" jeweils durch die Wörter „Darstellung in Textform" ersetzt.

2. In § 53 Abs. 2 Satz 1 und 2 wird jeweils das Wort „schriftlich" durch die Wörter „in Textform" ersetzt.

Artikel 24

Änderung der Börsenzulassungs-Verordnung

In § 45 Nr. 1 der Börsenzulassungs-Verordnung in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2832), geändert durch Artikel 3 Abs. 3 des Gesetzes vom 21. Dezember 2000 (BGBl. I S. 1857), werden die Wörter „schriftliche Darstellung“ und „schriftlichen Darstellung“ jeweils durch die Wörter „Darstellung in Textform“ ersetzt.

Artikel 25

Änderung des Gesetzes über Kapitalanlagegesellschaften

In § 19 Abs. 6 Satz 2 des Gesetzes über Kapitalanlagegesellschaften in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2726), das zuletzt durch Artikel 17 des Gesetzes vom 26. Juni 2001 (BGBl. I S. 1310) geändert worden ist, werden die Wörter „schriftliche Werbung“ durch die Wörter „Werbung in Textform“ ersetzt.

Artikel 26

Änderung des Umwandlungsgesetzes

Das Umwandlungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3210; 1995 I S. 428), zuletzt geändert durch Artikel 5 des Gesetzes vom 18. Januar 2001 (BGBl. I S. 123), wird wie folgt geändert:

1. In § 89 Abs. 2, § 182 Satz 1, §§ 216, 230 Abs. 1, § 256 Abs. 3 und § 260 Abs. 1 Satz 1 wird jeweils das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

2. § 267 wird wie folgt geändert:
   a) In Absatz 1 Satz 1 wird das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.
   b) In Absatz 2 Satz 1 wird das Wort „schriftlichen“ gestrichen.

Artikel 27

Änderung des Aktiengesetzes

Das Aktiengesetz vom 6. September 1965 (BGBl. I S. 1089), zuletzt geändert durch Artikel 8 Abs. 11 des Gesetzes vom 27. April 2001 (BGBl. I S. 751), wird wie folgt geändert:

1. In § 109 Abs. 3 wird das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

2. In § 121 Abs. 4 Satz 1 werden nach den Wörtern „einberufen werden“ die Wörter „ , wenn die Satzung nichts anderes bestimmt“ eingefügt.

3. § 122 Abs. 1 Satz 2 wird wie folgt gefasst:

   „Die Satzung kann das Recht, die Einberufung der Hauptversammlung zu verlangen, an eine andere Form und an den Besitz eines geringeren Anteils am Grundkapital knüpfen.“

Artikel 28

Änderung des Gesetzes betreffend die Gesellschaften mit beschränkter Haftung

Das Gesetz betreffend die Gesellschaften mit beschränkter Haftung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4123-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 des Gesetzes vom 18. Januar 2001 (BGBl. I S. 123), wird wie folgt geändert:

1. In § 47 Abs. 3 werden die Wörter „schriftlichen Form“ durch das Wort „Textform“ ersetzt.

2. In § 48 Abs. 2 wird das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

Artikel 29

Änderung des Gesetzes über das Kreditwesen

In § 23a Abs. 1 Satz 2 und Abs. 2 des Gesetzes über das Kreditwesen in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), das zuletzt durch Artikel 3 § 36 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266) geändert worden ist, wird jeweils das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

Artikel 30

Änderung des Versicherungsaufsichtsgesetzes

In § 53c Abs. 3a Satz 1 Nr. 5 und Abs. 3b Satz 4 des Versicherungsaufsichtsgesetzes in der Fassung der Bekanntmachung vom 17. Dezember 1992 (BGBl. 1993 I S. 2), das zuletzt durch Artikel 10 des Gesetzes vom 26. Juni 2001 (BGBl. I S. 1310) geändert worden ist, wird jeweils das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

Artikel 31

Änderung des Gesetzes über den Versicherungsvertrag

In § 5 Abs. 1 und Abs. 2 Satz 1, § 5a Abs. 1 Satz 1, §§ 37 und 158e Abs. 1 Satz 2 des Gesetzes über den Versicherungsvertrag in der im Bundesgesetzblatt Teil III, Gliederungsnummer 7632-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 38 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266) geändert worden ist, wird jeweils das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

Artikel 32

Änderung des Nachweisgesetzes

Nach § 2 Abs. 1 Satz 2 des Nachweisgesetzes vom 20. Juli 1995 (BGBl. I S. 946), das zuletzt durch Artikel 7 des Gesetzes vom 24. März 1999 (BGBl. I S. 388) geändert worden ist, wird folgender Satz eingefügt:

„Der Nachweis der wesentlichen Vertragsbedingungen in elektronischer Form ist ausgeschlossen."

Artikel 33

Änderung des Pflichtversicherungsgesetzes

In § 3 Nr. 7 des Pflichtversicherungsgesetzes in der Fassung der Bekanntmachung vom 5. April 1965 (BGBl. I S. 213), das zuletzt durch die Verordnung vom 22. Oktober 2000 (BGBl. I S. 1484) geändert worden ist, wird das Wort „schriftlich" durch die Wörter „in Textform" ersetzt.

Artikel 34

Rückkehr zum einheitlichen Verordnungsrang

Die auf den Artikeln 15 und 24 beruhenden Teile der dort geänderten Rechtsverordnungen können auf Grund der jeweils einschlägigen Ermächtigung durch Rechtsverordnung geändert werden.

Artikel 35

Inkrafttreten

Dieses Gesetz tritt am ersten Tag des auf die Verkündung folgenden Kalendermonats in Kraft.

Die verfassungsmäßigen Rechte des Bundesrates sind gewahrt.

Das vorstehende Gesetz wird hiermit ausgefertigt und wird im Bundesgesetzblatt verkündet.

Berlin, den 13. Juli 2001

Der Bundespräsident
Johannes Rau

Der Bundeskanzler
Gerhard Schröder

Die Bundesministerin der Justiz
Däubler-Gmelin

IT-Grundschutzhandbuch in Auszügen

Inhaltsverzeichnis

3.6	Computer-Virenschutzkonzept	4.4	Schutzschränke
3.7	Kryptokonzept	4.5	Häuslicher Arbeitsplatz
3.8	Behandlung von Sicherheitsvorfällen	4.6	Rechenzentrum
3.9	Hard- und Software-Management		

5.	Nicht vernetzte IT-Systeme / Clients	6.	Vernetzte IT-Systeme
5.1	DOS-PC (ein Benutzer)	6.1	Servergestütztes Netz
5.2	PCs mit wechselnden Benutzern	6.2	Unix-Server
5.3	Tragbarer PC	6.3	Peer-to-Peer-Netz
5.4	Unix-System	6.4	Windows NT Netz
5.5	Windows NT - PC	6.5	Novell Netware 3.x
5.6	Windows 95 - PC	6.6	Novell Netware 4.x
5.99	Allgemeines nicht vernetztes IT-System	6.7	Heterogene Netze
		6.8	Netz- und Systemmanagement

7.	Datenübertragungseinrichtungen	8.	Telekommunikation
7.1	Datenträgeraustausch	8.1	TK-Anlage
7.2	Modem	8.2	Faxgerät
7.3	Firewall	8.3	Anrufbeantworter
7.4	E-Mail	8.4	LAN-Anbindung eines IT-Systems über ISDN
7.5	WWW-Server	8.5	Faxserver
7.6	Remote Access	8.6	Mobiltelefon
7.7	Lotus Notes		

9.	Sonstige IT-Komponenten
9.1	Standardsoftware
9.2	Datenbanken

9.3 Telearbeit

Maßnahmenkataloge	Gefährdungskataloge
M 1 Infrastruktur	G 1 Höhere Gewalt
M 2 Organisation	G 2 Organisatorische Mängel
M 3 Personal	G 3 Menschliche Fehlhandlungen
M 4 Hardware/Software	G 4 Technisches Versagen
M 5 Kommunikation	G 5 Vorsätzliche Handlungen
M 6 Notfallvorsorge	

G 1 Gefährdungskatalog Höhere Gewalt

G 1.1 Personalausfall

G 1.2 Ausfall des IT-Systems

G 1.3 Blitz

G 1.4 Feuer

G 1.5 Wasser

G 1.6 Kabelbrand

G 1.7 Unzulässige Temperatur und Luftfeuchte

G 1.8 Staub, Verschmutzung

G 1.9 Datenverlust durch starke Magnetfelder

G 1.10 Ausfall eines Weitverkehrsnetzes

G 1.11 Technische Katastrophen im Umfeld

G 1.12 Beeinträchtigung durch Großveranstaltungen

G 1.13 Sturm

G 1.1 Personalausfall

Durch Krankheit, Unfall, Tod oder Streik kann ein nicht vorhersehbarer Personalausfall entstehen. Desweiteren ist auch der Personalausfall bei einer regulären

Beendigung des Arbeitsverhältnisses zu berücksichtigen, insbesondere wenn die Restarbeitszeit z. B. durch einen Urlaubsanspruch verkürzt wird.
In allen Fällen kann die Konsequenz sein, dass entscheidende Aufgaben aufgrund des Personalausfalls im IT-Einsatz nicht mehr wahrgenommen werden. Dies ist besonders dann kritisch, wenn die betroffene Person im IT-Bereich eine Schlüsselstellung einnimmt und aufgrund fehlenden Fachwissens anderer nicht ersetzt werden kann. Störungen des IT-Betriebs können die Folge sein.
Ein Personalausfall kann zusätzlich einen empfindlichen Verlust von Wissen und Geheimnissen nach sich ziehen, der die nachträgliche Übertragung der Tätigkeiten auf andere Personen unmöglich macht.

Beispiele:
Aufgrund längerer Krankheit blieb der Netzadministrator vom Dienst fern. In der betroffenen Firma lief das Netz zunächst fehlerfrei weiter. Nach zwei Wochen jedoch war nach einem Systemabsturz niemand in der Lage, den Fehler zu beheben. Dies führte zu einem Ausfall des Netzes über mehrere Tage.
Während des Urlaubs des Administrators muss für Datensicherungszwecke auf die Backupbänder im Datensicherungstresor zurückgegriffen werden. Der Zugangscode zum Tresor wurde erst kürzlich geändert und ist nur dem Administrator bekannt. Erst nach mehreren Tagen konnte die Datenrestaurierung durchgeführt werden, da der Aufenthaltsort des Administrators zuerst ermittelt werden musste.

M 1 Maßnahmenkatalog Infrastruktur

M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
M 1.2 Regelungen für Zutritt zu Verteilern
M 1.3 Angepaßte Aufteilung der Stromkreise
M 1.4 Blitzschutzeinrichtungen
M 1.5 Galvanische Trennung von Außenleitungen
M 1.6 Einhaltung von Brandschutzvorschriften
M 1.7 Handfeuerlöscher
M 1.8 Raumbelegung unter Berücksichtigung von Brandlasten

M 1.9 Brandabschottung von Trassen

M 1.10 Verwendung von Sicherheitstüren und -fenstern

M 1.11 Lagepläne der Versorgungsleitungen

M 1.12 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

M 1.13 Anordnung schützenswerter Gebäudeteile

M 1.14 Selbsttätige Entwässerung

M 1.15 Geschlossene Fenster und Türen

M 1.16 Geeignete Standortauswahl

M 1.17 Pförtnerdienst

M 1.18 Gefahrenmeldeanlage

M 1.19 Einbruchsschutz

M 1.20 Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht

M 1.21 Ausreichende Trassendimensionierung

M 1.22 Materielle Sicherung von Leitungen und Verteilern

M 1.23 Abgeschlossene Türen

M 1.24 Vermeidung von wasserführenden Leitungen

M 1.25 Überspannungsschutz

M 1.26 Not-Aus-Schalter

M 1.27 Klimatisierung

M 1.28 Lokale unterbrechungsfreie Stromversorgung

M 1.29 Geeignete Aufstellung eines IT-Systems

M 1.30 Absicherung der Datenträger mit TK-Gebührendaten

M 1.31 Fernanzeige von Störungen

M 1.32 Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern

M 1.33 Geeignete Aufbewahrung tragbarer PCs bei mobilem Einsatz

M 1.34 Geeignete Aufbewahrung tragbarer PCs im stationären Einsatz

M 1.35 Sammelaufbewahrung mehrerer tragbarer PCs

M 1.36 Sichere Aufbewahrung der Datenträger vor und nach Versand

M 1.37 Geeignete Aufstellung eines Fax-Gerätes

M 1.38 Geeignete Aufstellung eines Modems

M 1.39 Verhinderung von Ausgleichsströmen auf Schirmungen

M 1.40 Geeignete Aufstellung von Schutzschränken

M 1.41 Schutz gegen elektromagnetische Einstrahlung

M 1.42 Gesicherte Aufstellung von Novell Netware Servern

M 1.43 Gesicherte Aufstellung von ISDN-Routern

M 1.44 Geeignete Einrichtung eines häuslichen Arbeitsplatzes

M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

M 1.46 Einsatz von Diebstahl-Sicherungen

M 1.47 Eigener Brandabschnitt

M 1.48 Brandmeldeanlage

M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum

M 1.50 Rauchschutz

M 1.51 Brandlastreduzierung

M 1.52 Redundanzen in der technischen Infrastruktur

M 1.53 Videoüberwachung

M 1.54 Brandfrühesterkennung / Löschtechnik

M 1.55 Perimeterschutz

M 1.56 Sekundär-Energieversorgung

M 1.57 Aktuelle Infrastruktur- und Baupläne

M 1.58 Technische und organisatorische Vorgaben für Serverräume

M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften

Verantwortlich für Initiierung: Leiter Beschaffung, Planer

Verantwortlich für Umsetzung: Bauleiter, Errichterfirma

Für nahezu alle Bereiche der Technik gibt es Normen bzw. Vorschriften, z. B. DIN, VDE, VDMA, Richtlinien des VdS. Diese Regelwerke tragen dazu bei, daß technische Einrichtungen ein ausreichendes Maß an Schutz für den Benutzer und Sicherheit für den Betrieb gewährleisten.

Bei der Planung und Errichtung von Gebäuden, bei deren Umbau, beim Einbau technischer Gebäudeausrüstungen (z. B. interne Versorgungsnetze wie Telefon-

oder Datennetze) und bei Beschaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften unbedingt zu beachten.

Ergänzende Kontrollfragen:
Werden VDE-Vorschriften bei Ausschreibungen, Bestellungen oder Beschaffungen berücksichtigt?

DANIEL WALTHER LEBENSLAUF

Persönliche Daten

Geboren am	10.11.1974, Frankfurt/Main
Familienstand	verheiratet mit Brigitte Walther geb. Jenisch

Schule, Zivildienst

09/1981-07/1986	Peter-Petersen-Grundschule, Frankfurt/Main
09/1985-06/1994	Ziehengymnasium, Frankfurt/Main Abitur-Note 1,3 (Leistungskurse Mathematik/Physik)
08/1994-10/1995	Zivildienst Mobiler Sozialer Hilfsdienst, Hauspflegeverein e.V., Frankfurt/Main

Studium

10/1995-03/2000 Studium der Wirtschaftsinformatik an der Technischen Universität Darmstadt

Diplomarbeit: Ein Sicherheitskonzept zur Einführung von SAP R/3 bei der Lufthansa AG

Informatikspezialisierungen Datenbanken und Betriebssysteme (24 SWS)
Vertiefungsfach Zivil- und Arbeitsrecht (8 SWS)

Abschlußnote: sehr gut

10/1995-08/2001 Studium der Mathematik an der Technischen Universität Darmstadt

Diplomarbeit: Realisierung einer Webapplikation für lineare Optimierungen nach der M-Methode

Schwerpunkt Informatik

Abschlußnote: gut

05/2000-07/2003 Promotion am Institut für Betriebswirtschaftslehre der TU-Darmstadt, Lehrstuhl für Wirtschaftsinformatik

Thema: Wirtschaftlichkeit von Zertifizierungsstellen in Deutschland

Beauftragt mit dem Konzept und dem Aufbau eines Intranets zur Verbesserung des Workflows und der Aktualität des Webauftritts des Fachbereichs (PHP/mySQL).

Lehraufträge für
- Grundlagen der Datenverarbeitung und Programmierung (Übung) [in C/C++]
- Wirtschaftsinformatikpraktikum
- SAP-Praktikum

Betreuung von
- Seminar Wirtschaftsinformatik
- Seminar Bankinformatik
- Einführung in die Wirtschaftsinformatik
- Betreuung von Studien- und Diplomarbeiten
  (Wirtschaftlichkeitsaspekte, Konzepte und Implementierung von E-Billing-Systemen, Trackingsystemen, Fondverwaltung, Zertifizierungsstellen, Risikoanalyse, E-Commerce)

Auszeichnungen

05/1989	Kreissieger Frankfurt/Main des Mathematikwettbewerbes (2. Runde)
03/1993	4. Platz Einzelwettbewerb Tag der Mathematik in Bensheim (182 Teilnehmer) 3. Platz Gruppenwettbewerb Tag der Mathematik in Bensheim